| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| **A** | Is privacy a constitutionally protected right in your Economy? | Yes, in 2009 two amendments to constitutional articles 16 and 73 were published with the purpose of setting the *recognition to the right of personal data protection as fundamental and autonomous* (article 16 second paragraph) and to *provide the Federal Congress with the power to rule in matters related to personal data held by private parties and its protections* (article 73).<br><br>Likewise, in 2014, article 6 of the Mexican Constitution was amended to recognize the data protection right and to provide the existence of an autonomous federal data protection authority.<br><br>Political Constitution of the United Mexican States (*Constitución Política de los Estados Unidos Mexicanos*, text available only in Spanish): | *Article 6 […]*<br>*A. […]*<br>*II. Information regarding private life and personal data shall be protected according to law and with the exceptions established therein.*<br>*. […]*<br>*VIII.* The Federation shall establish an autonomous, specialized, impartial and collegiate agency. It must have a legal personality; own assets; full technical, managerial and decision power over its budget and internal organization; and shall be responsible for guaranteeing the fulfillment of the right of access to public information and the protection of personal data held by public agencies (obligated subjects), according to the terms established by law. *[…]*<br><br>*Article 16 […]*<br>All people have the right to enjoy protection on his personal data, and to access, correct and cancel such data. All people have the right to oppose the disclosure of his data, | N/A | Enacted |

[1] *Note here the legislation, rule, code, framework or other privacy protection scheme. Where possible please provide the URL for the website where the legislation or arrangement is available.*

[2] *Insert the full text or summary of the provisions of your privacy protection scheme(s) that correspond to the APEC Privacy Principles identified in the column titled "APEC Principle/ Commentary".*

[3] *Sanctions should include the nature of the remedies available, the means by which they are obtained, and by whom (for example, government, local law enforcement, private right of action, etc.).*

[4] *Identify areas where the practice and the intent of the principle need further consideration; and identify the status of the economies' practice, for example enacted, introduced, draft. If your legislation, rule, code, framework or other privacy protection scheme is at the drafting or proposal stage and has not yet been enacted or implemented, please indicate here and provide any other useful comments."*

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm | according to the law. The law shall establish exceptions to the criteria that rule the handling of data, due to national security reasons, law and order, public security, public health, or protection of third party's rights. […]<br><br>Article 73. The congress has the power: […]<br>XXIX-O. To regulate in connection with the protection of personal data held by private parties. […] | | |
| **B** | If not, what other available legislation deals with privacy or confidentiality of personal information. | A. Federal Consumer Protection Law (*Ley Federal De Protección al Consumidor*).<br><br>https://www.diputados.gob.mx/LeyesBiblio/ref/lfpc.htm<br><br>B. Federal Law on Protection of Personal Data held by Private Parties *(Ley Federal de Protección de Datos Personales en Posesión de los Particulares)*, published in the Federal Official Gazette on July 5th, 2010.<br><br>http://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp.htm<br><br>C. Regulations to the Federal Law on Protection of Personal Data held by Private Parties (*Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*), published in the | N/A | N/A | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | Federal Official Gazette on December 21st, 2011<br><br>http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf<br><br>http://inicio.inai.org.mx/English_Section_Documents/LFPDPPP%20REG%20ENG.pdf<br><br>D. Parameters for personal data self-regulation (Parámetros de autorregulación en materia de protección de datos personales). Federal Official Gazette on May 29, 2014.<br><br>http://www.dof.gob.mx/nota_detalle.php?codigo=5346597&fecha=29/05/2014<br><br>E. Rules of operation of the Registry of Self-Regulation Schemes (*Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante).* Federal Official Gazette on February 18, 2015.<br><br>https://www.dof.gob.mx/nota_detalle.php?codigo=5382543&fecha=18/02/2015<br><br>F. General Law on Protection of Personal Data Held by Obligated Parties –federal and local authorities- (*Ley General de Protección de Datos Personales en* | | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | *Posesión de Sujetos Obligados),* published in the Federal Official Gazette on January 26th, 2017.<br><br>http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017<br><br>http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf<br><br>G. Guidelines to the General Law on Protection of Personal Data Held by Obligated Parties *(Lineamientos Generales de Protección de Datos Personales para el Sector Público),* published in the Federal Official Gazette on January 26th, 2018, available at:<br><br>http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf and modifications<br><br>https://home.inai.org.mx/wp-content/documentos/AcuerdosDelPleno/ACT-PUB-11-11-2020.05.pdf<br><br>And ACT-PUB/09/02/2022.07: http://home.inai.org.mx/wp-content/documentos/AcuerdoDelPleno/ACT-PUB-09-02-2022.07.zip, www.dof.gob.mx/2022/INAI/ACT-PUB-09-02-2022-07.zip; and http://dof.gob.mx/nota_detalle.php?codigo=5643872&fecha=25/02/2022. | | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | H. Federal Law of Transparency and Access to Public Information (*Ley Federal de Transparencia y Acceso a la Información Pública*), published in the Federal Official Gazette on May 9th, 2016<br>https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_200521.pdf<br>I. Federal Tax Code (*Código Fiscal De La Federación*)<br>https://www.diputados.gob.mx/LeyesBiblio/pdf/CFF.pdf<br>J. General Law of Electoral Institutions and Procedures (*Ley General de Instituciones y Procedimientos Electorales*)<br>http://www.diputados.gob.mx/LeyesBiblio/ref/lgipe.htm<br>K. Federal Public Administration Services Law (*Ley del Servicio Profesional de Carrera en la Administración Pública Federal*)<br>http://www.diputados.gob.mx/LeyesBiblio/ref/lspcapf.htm | | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | L. Copyright Act[5] (*Ley Federal del Derecho de Autor*)[6]<br>http://www.diputados.gob.mx/LeyesBiblio/ref/lfda.htm<br>M. Credit Information Company Act (*Ley para Regular las Sociedades de Información Crediticia*)<br>http://www.diputados.gob.mx/LeyesBiblio/ref/lrsic.htm<br>• AI.MX private Trustmark | | | |
| **1** | ***I Preventing Harm***<br>**(Ref. Para. 20)**<br>Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal | Federal Law on Protection of Personal Data held by Private Parties. | Article 7. Personal data must be collected and processed in a lawful manner in accordance with the provisions established by this Law and other applicable regulations.<br>Personal data must not be obtained through deceptive or fraudulent means.<br>In all processing of personal data, it is presumed that there is a reasonable expectation of privacy, understood as the trust any one person places in another for personal data provided to be treated pursuant to any agreement of the parties in the terms established by this Law. | Article 63.- The following acts carried out by the data controller are violations of the Federal Law on Protection of Personal Data held by Private Parties :<br>I. Failure to satisfy the data owner's request for personal data access, rectification, cancellation or objection without well-founded reason, in the terms of this Law ;<br>II. Acting negligently or fraudulently in processing and responding to requests for personal data access, rectification, cancellation or objection; | Enacted |

[5] *Not necessarily copyrights*
[6] *About the protection of Data bases*

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | information. | Regulations to the Federal Law on Protection of Personal Data held by Private Parties | Article 44. The principle of loyalty establishes the obligation to process personal data giving priority to the protection of the interests of the data subject and the reasonable expectation of privacy, as provided in Article 7 of the Law. Misleading or fraudulent means may not be used to collect and process personal data. It will be considered that the behavior is fraudulent or misleading when:<br>I. There is fraud, bad faith or negligence in the information provided to the data subject about the processing;<br>II. The reasonable expectation of privacy of the data subject referred to in Article 7 of the Law is violated, or<br>III. The purposes were not established in the privacy notice. | III. Fraudulently declaring the inexistence of personal data where such exists in whole or in part in the databases of the data controller;<br>IV. Processing personal data in violation of the principles established in this Law;<br>V. Omitting, in the privacy notice, any or all of the items referred to in Article 16 of this Law;<br>VI. Maintaining inaccurate personal data when such action is attributable to the data controller, or failing to perform legally due rectifications or cancellations where the data owner's rights are affected;<br>VII. Failure to comply with the notice referred to in section I of Article 64;<br>VIII. Breaching the duty of confidentiality established in Article 21 of this Law;<br>IX. Materially changing the original data processing purpose, without observing the provisions of Article 12;<br>X. Transferring data to third parties without providing them with the privacy notice containing the limitations to which the data owner has conditioned data disclosure;<br>XI. Compromising the security of databases, sites, programs or equipment, | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | | where attributable to the data controller;<br>XII. Carrying out the transfer or assignment of personal data outside of the cases where it is permitted under this Law;<br>XIII. Collecting or transferring personal data without the express consent of the data owner, in the cases where this is required;<br>XIV. Obstructing verification actions of the authority;<br>XV. Collecting data in a deceptive and fraudulent manner;<br>XVI. Continuing with the illegitimate use of personal data when the Institute or the data owners have requested such use be ended;<br>XVII. Processing personal data in a way that affects or impedes the exercise of the rights of access, rectification, cancellation and objection set forth in Article 16 of the Political Constitution of the United Mexican States;<br>XVIII. Creating databases in violation of the provisions of Article 9, second paragraph, of this Law, and<br>XIX. Any breach by the data controller of the obligations pertaining thereto as established in the provisions of this Law. | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | | Article 64.- Violations to this Federal Law on Protection of Personal Data held by Private Parties will be punished by the National Institute of Transparency, Access to Information and Data Protection (INAI) as follows:<br>I. A warning instructing the data controller to carry out the actions requested by the data owner, under the terms established by this Law, in the cases described in section I of the preceding article;<br>II. A fine from 100 to 160,000 days of the Mexico City minimum wage, in the cases described in sections II to VII of the preceding article;<br>III. A fine from 200 to 320,000 days of the Mexico City minimum wage, in the cases described in sections VIII to XVIII of the preceding article; and<br>IV. In the event of repeated occurrences of the violations described in the preceding paragraphs, an additional fine will be imposed from 100 to 320,000 days of the current Mexico City minimum wage.<br>With regard to violations committed in processing sensitive data, sanctions may be increased up to double the | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | | established amounts.<br><br>Article 65. The INAI will ground its decisions in law and fact, considering:<br><br>I. The nature of the data;<br><br>II. The evident impropriety of the refusal of the data controller to perform the actions requested by the data owner in the terms of this Law;<br><br>III. The intentional or unintentional nature of the action or omission constituting the violation;<br><br>IV. The financial position of the data controller, and<br><br>V. Recurrence. | |
| | | General Law on Protection of Personal Data Held by Obligated Parties. | Article 17. The processing of personal data by the data controller must be carried out within the scope of the faculties and attributions conferred to the data controller under applicable regulations.<br><br>Article 18. All processing of personal data by the data controller must be justified as undertaken for specific, lawful, explicit and legitimate purposes relating to the attributions vested in the data controller under applicable regulations. | Article 163. The following are causes giving rise to sanction as a result of non-compliance with the obligations as set forth in this Law: **I.** Acting with negligence, dolus or bad faith in the handling of requests for exercise of ARCO rights; **II.** Failing to comply with the time periods contemplated in this Law to respond to requests to exercise ARCO rights or to uphold the relevant right; **III.** Using, | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | The data controller may process personal data for purposes other than those set forth in the privacy notice, provided the data controller has the required attributions to do so as conferred by law and has obtained the data owner's consent, unless a person reported as missing is concerned, this as provided in this Law and other applicable provisions on the matter.<br><br>Article 19. The data controller must not obtain and process personal data by deceitful or fraudulent means, prioritizing the protection of the data owner's interests and the reasonable expectation of privacy. | deleting, disclosing, concealing, altering, distorting, destroying or rendering personal data useless, in whole or in part, and improperly, that are held under the party's custody or to which he/she has access or has knowledge of by reason of his/her job, office or commission; **IV.** Willfully processing personal data in contravention of the principles and duties established in this Law; **V.** Not having a privacy notice, or else, omitting in the same any one of the elements referred to in article 27 of this Law, as the case may be, and other applicable provisions on the matter; **VI.** Classifying, with dolus or negligence, personal data as confidential without these meeting the characteristics set forth in applicable laws. The sanction will only be warranted as a result of a prior final determination that is not subject to appeal regarding the classification criterion of the personal data; **VII.** Failing to comply with the duty of confidentiality established in article 42 of this Law; **VIII.** Failing to establish the security measures as are set forth in articles 31, 32 and 33 | |
| | | General Guidelines of Protection of Personal Data Held by Obligated Parties. | Article 11 defines what must be understood as *deceptive means*; when it is considered that the data controller is processing personal data favoring the interests of the data subject and the meaning of the term *reasonable expectation of privacy*. | | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | | of this Law; **IX.** When the personal data are violated are a result of the failure to implement the security measures as are set forth in articles 31, 32, and 33 of this Law; X**.** Transferring personal data in contravention of the provisions of this Law; **XI.** Obstructing verification action conducted by the authority; **XII.** Creating personal data bases in contravention of the provisions of article 5 of this Law; **XIII.** Failing to comply with the resolutions issued by the Institute and the Guarantor bodies; and **XIV.** Failing to submit the annual report and other reports referred to in article 44, section VII of the General Law on Transparency and Access to Public Information, or else to do so extemporaneously.<br><br>Causes giving rise to responsibility contemplated in sections I, II, IV, VI, X, XII and XIV, as well as recidivism in the actions contemplated in the remaining sections of this article, will be considered to be grave for administrative sanctioning purposes. | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | | In the event the presumed infringement is committed by a member of a political party, the investigation, and such being the case, sanction will be conducted and applied by the competent electoral authority.<br>Monetary sanctions cannot be settled with public funds.<br><br>Additionally, Articles 164 y 165, which, in general provide that the conducts referred to in the preceding article will be reported to the competent authority for it – for example, the internal control body - to impose or enforce the sanction.<br><br>These sanctions are independent from any civil, criminal, civil or other liabilities which may arise from the same actions, which may be imposed by the competent authorities and by the applicable laws. | |
| **2** | ***II Notice***<br>**(Ref. Para. 21-23)**<br>Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information | Federal Law on Protection of Personal Data held by Private Parties. | Article 3.- For purposes of this Law, the following definitions will apply:<br><br>Privacy Notice: Document in physical, electronic or any other format, generated by the data controller that is made available to | Articles 63, 64 and 65 of Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | that should include:<br>a) the fact that personal information is being collected;<br>b) the purposes for which personal information is collected;<br>c) the types of persons or organizations to whom personal information might be disclosed;<br>d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information;<br>e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.<br>All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.<br>It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information. | | the data owner prior to the processing of his personal data, in accordance with Article 15 of this Law.<br><br>Article 8.- All processing of personal data will be subject to the consent of the data owner except as otherwise provided by this Law.<br><br>Consent will be express when such is communicated verbally, in writing, by electronic or optical means or via any other technology, or by unmistakable indications.<br><br>It will be understood that the data owner tacitly consents to the processing of his data when, once the privacy notice has been made available to him, he does not express objection.<br><br>Financial or asset data will require the express consent of the data owner, except as provided in Articles 10 and 37 of this Law.<br><br>Consent may be revoked at any time without retroactive effects being attributed thereto. For revocation of consent, the data controller must, in the privacy notice, establish the mechanisms and procedures for such action<br><br>Article 14. - The data controller shall ensure compliance with the personal data protection principles | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller. The data controller must take all necessary and sufficient action to ensure that the privacy notice given to the data owner is respected at all times by it or by any other parties with which it has any legal relationship.<br><br>Article 15. - The data controller will have the obligation of providing data owners with information regarding what information is collected on them and why, through the privacy notice.<br><br>Article 16.- The privacy notice must contain at least the following information:<br><br>I. The identity and domicile of the data controller collecting the data;<br>II. The purposes of the data processing;<br><br>III. The options and means offered by the data controller to the data owners to limit the use or disclosure of data;<br><br>IV. The means for exercising rights of access, rectification, cancellation | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | or objection, in accordance with the provisions of this Law;<br><br>V. Where appropriate, the data transfers to be made, and<br><br>VI. The procedure and means by which the data controller will notify the data owners of changes to the privacy notice, in accordance with the provisions of this Law. For sensitive personal data, the privacy notice must expressly state that it is dealing with this type of data.<br><br>Article 17. The privacy notice must be made available to data owners through print, digital, visual or audio formats or any other technology, as follows:<br><br>I. Where personal data has been obtained personally from the data owner, the privacy notice must be provided at the time the data is collected, clearly and unequivocally, through the format by which collection is carried out, unless the notice has been provided prior;<br><br>II. Where personal data are obtained directly from the data owner by any electronic, optical, audio or visual means, or through any other technology, the data controller must immediately provide the data owner with at least the information referred to in sections I and II of the preceding | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | article, as well as provide the mechanisms for the data owner to obtain the full text of the privacy notice.<br><br>Article 18. Where data has not been obtained directly from the data owner, the data controller must notify him of the change in the privacy notice. The provisions of the preceding paragraph are not applicable where processing is done for historical, statistical or scientific purposes. Where it is impossible to provide the privacy notice to the data owner or where disproportionate effort is involved considering the number of data owners, or the age of the data, with the authorization of the Institute, the data controller may implement compensatory measures in the terms of the Regulation for this Law.<br><br>Article 33. The obligation to provide access to information will be fulfilled when the personal data is made<br><br>available to the data owner; or, by issuing uncertified copies, electronic documents or any other means established by the data controller in the privacy notice.<br><br>In the event that the data owner requests access to data from a person or entity who he presumes is the data controller and said person | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | or entity proves not to be such, it will be sufficient for said person or entity to so indicate to the data owner by any of the means referred to in the preceding paragraph, for the request to be considered properly fulfilled.<br><br>Article 36. Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing.<br><br>Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his data; moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data. | | |
| | | Regulations to the Federal Law on Protection of Personal Data held by Private Parties | Article 23. The data controller must bring to the attention of the data subject the information related to the existence and main characteristics of the processing to which his personal data will be submitted, through a privacy notice, pursuant to the Law and this Regulations.<br><br>Article 24. The privacy notice must be simple, with the necessary information, written in a clear and understandable language, and with a | Articles 63, 64 and 65 of Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | structure and design that facilitates its understanding.<br><br>Article 25. For the divulging of privacy notices, the data controller may use physical or electronic formats, verbal means or any other technology, provided it complies with the duty to inform the data subject.<br><br>Article 26. A privacy notice must contain the items referred to in Articles 8, 15, 16, 33, and 36 of the Law, as well as those established in the guidelines referred to in Article 43(III) of the Law.<br><br>Article 27. As provided in Article 17(II) of the Law, when personal data is obtained directly from the data subject, the data controller must immediately provide at least the following information: I. The identity and address of the data controller; II. The purposes of the processing, and III. The mechanisms offered by the data controller so that the data subject will be aware of the privacy notice in accordance with Article 26 of these Regulations. The immediate divulging of the above information does not exempt the data controller from the obligation to provide mechanisms for the data subject to become aware of the content of the privacy notice, pursuant to Article 26 of these Regulations.<br><br>Article 28. The data controller may bring a privacy notice to the attention | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | of the data subject, as provided in the previous Article, when it obtains personal data by printed means, provided the space used to obtain the personal data is minimal and limited so that the personal data obtained is also the minimum.<br><br>Article 29. When personal data is obtained indirectly from the data subject, the data controller must observe the following in order to bring the privacy notice to the attention of the data subject: I. When the personal data are processed for the purpose contemplated in the consent to transfer or have been obtained from a public access source, the privacy notice shall be made known in the first contact with the data subject, or II. When the data controller wishes to use the data for a purpose different from that consented to, in other words, there will be a change of purpose, the privacy notice must be made known prior to the use of the data.<br><br>Article 30. Among the purposes of processing referred to in Article 16(II) of the Law, as applicable, there must be included those concerning processing for marketing, advertising, or commercial exploration. The above is without prejudice to current law which regulates processing for the purposes set out in the previous paragraph when this contemplates higher protection for the data subject | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | than that provided in the Law and these Regulations.<br><br>Article 31. To show that a privacy notice has been given in accordance with the principle of information, the burden of proof shall always rest upon the data controller.<br><br>Article 32. In accordance with Article 18, third paragraph, of the Law, when it is impossible to communicate the privacy notice to the data subject or this requires disproportionate efforts given the number of data subjects or the age of the data, the data controller may implement compensatory measures using mass communication media in accordance with the guidelines issued by the Institute and published in the Federal Official Gazette under which it is possible to use the measures established in Article 35 of these Regulations. The cases not included in the guidelines issued by the Institute shall require the express authorization of the latter, prior to the implementation of the compensatory measure, in accordance with the procedure established in Articles 33 and 34 of these Regulations.<br><br>Article 33. The procedure to obtain authorization from the Institute for the use of compensatory measures using mass communication media to which the previous Article refers, shall always be initiated at the request of the data controller. The | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | data controller shall submit the request directly to the Institute or by any other means that the latter has authorized for this purpose. The request shall contain the following information:<br><br>I. The name of the data controller making the application, and as applicable, of its representative, as well as a copy of the official identification proving legal status and the original for comparison. In the case of a representative, a copy of the document proving his right to represent the data controller must be submitted, as well as the original for comparison;<br><br>II. Address to receive notifications and name of person authorized to receive them;<br><br>III. The processing to which it is intended to apply the compensatory measure and its principal features, such as purpose; type of personal data processed; if transfers are to take place; details of the data subjects, among them age, geographic location, educational and socio-economic level, among others;<br><br>IV. Causes or justification for the impossibility of bringing a privacy notice to the attention of the data subjects or the disproportionate efforts that this would require. The data controller shall state the number of data subjects involved, age of the | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | data, whether or not there is direct contact with the data subjects, and their economic situation;<br><br>V. Type of compensatory measure sought to be used and for what period of time it will be published;<br><br>VI. Proposed text for the compensatory measure, and<br><br>VII. Documents that the data controller considers necessary to submit to the Institute.<br><br>Article 34. The Institute shall have a period of ten days following receipt of the request for compensatory measures to issue its decision on the matter. If the Institute does not issue a decision within the period established, the compensatory measure request will be considered as authorized. Once the request is submitted by the data controller to the Institute, the latter shall weigh the disproportionate efforts to make known the privacy notice, taking the following into account:<br><br>I. The number of data subjects;<br><br>II. The age of the data;<br><br>III. The economic situation of the data controller;<br><br>IV. The geographic area and sector in which the data controller operates, and | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | V. The compensatory measure to be adopted. When weighing the request, if the Institute considers that the compensatory measure proposed does not comply with the principle of information, it may propose to the data controller the adoption of a compensatory measure different from that suggested by the data controller in its request. The proposal of the Institute shall be brought to the attention of the data controller so that it may take such action as it considers appropriate within a period of no more than five days, calculated from the day following that on which it received notification. If the data controller does not respond within the period mentioned in the previous paragraph, the Institute shall resolve the matter based on the file of the matter. When the Institute decides that the data controller does not justify the impossibility of bringing the privacy notice to the attention of the data subject or that this requires disproportionate efforts, the use of compensatory measures shall not be authorized. Any authorization given by the Institute shall be valid unless the circumstances under which the compensatory measure was authorized change.<br><br>Article 35. Mass communication compensatory measures must contain the information provided in Article 27 of these Regulations and | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | shall be made known by means of privacy notices published in any of the following media:<br><br>I. Newspapers with national circulation;<br><br>II. Local newspapers or specialized journals when it is proven that the data subjects reside in a particular federative entity or are part of a particular activity;<br><br>III. Web site of the data controller;<br><br>IV. On a hyperlink on an web site of the Institute, set up for this purposes, when the data controller does not have its own web site;<br><br>V. Informational posters;<br><br>VI. Information spots on the radio, or<br>VII. Other alternative mass communication media. | | |
| | | General Law on Protection of Personal Data Held by Obligated Parties. | Article 3. For the purposes of this Law the following definitions will apply:<br><br>Privacy Notice: Document generated by the data controller and made available to the data owner in physical, electronic or any other format upon of collection of the latter's personal data, in order to inform him/her on the purposes of their processing.<br><br>Article 26. The data controller must inform the data owner, by means of | Articles 163, 164 and 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | the privacy notice, on the existence and main characteristics of the processing to be given to his/her personal data, to enable him/her to make informed decisions in such regard.<br><br>As a general rule, the privacy notice must be disseminated on the electronic and physical means available to the data controller.<br><br>For the privacy notice to properly comply with its informative function, it must be drafted and structured in clear and simple terms.<br><br>Where it is impossible to make the privacy notice directly available to the data owner or if this requires a disproportionate effort, the data controller may implement alternate means of mass communication in accordance with the criteria issued on the matter by the National System for Transparency, Access to Public Information and Personal Data Protection.<br><br>Article 27. The privacy notice referred to in article 3, section II, will be made available to the data owner in two versions: a simplified and a complete version. The simplified version must contain the following information: **I.** Data owner's name; **II.** The purpose of the treatment for which the personal data are being | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | collected, specifying those that require the data owner's consent; **III.** Where personal data transfers requiring consent are to be made, information on the following must be provided: **a T**he governmental authorities, branches, entities, agencies and bodies of the three levels of government and the individuals and legal entities to whom personal data will be transferred, and **b) T**he purpose of such transfers. **IV.** The mechanisms and means available to allow the data owner, if so required, to express his/her opposition to the processing of his/her personal data for purposes and transfers of personal data requiring the data owner's consent; and **V.** The web page where the complete privacy notice may be consulted.<br><br>Availability of the privacy notice referred to in this article does not release the data controller from the obligation of providing the mechanisms allowing the data owner to become cognizant of the content of the privacy notice referred to in the following article.<br>The mechanisms and means referred to in section IV of this article must be made available to enable the data owner to express his/her opposition to the processing of his/her personal data for purposes or transfers requiring the data owner's | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | consent, prior to any such processing.<br>Article 28. The complete privacy notice must contain, in addition to that which is specified in the sections of the preceding article, at least the following information: **I.** The data controller's address; **II.** The personal data that will be subject to processing, identifying those that are sensitive; **III.** The legal grounds on which the data controller's authority to process rests; **IV.** The purposes of the processing for which the personal data are collected; with the specification of those requiring the data owner's consent; **V.** The available mechanisms, means and procedures to exercise ARCO rights; **VI.** The address of the Transparency Unit; and **VII.** The means to be used by the data controller to inform data owners on any changes in the privacy notice. | | |
| | | General Guidelines of Protection of Personal Data Held by Obligated Parties. | Articles 26 and 27, which provide the main features and aim of the privacy notice.<br><br>Articles 28 to 39, which stablish privacy notice characteristics, regarding means of diffusion, comprehensive and simplified versions of privacy notice particularities, mechanisms and means to express t refusal of data owner in the simplified privacy | Articles 163, 164 and 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | notice, consult of comprehensive privacy notice in the simplified privacy notice, information about personal data transfers in the comprehensive privacy notice, controller's address in in the comprehensive privacy notice, personal data in the comprehensive privacy notice, legal basis for processing in the comprehensive privacy notice. | | |
| **3** | ***III Collection Limitation*** **(Ref. Para. 24)** The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned. | Federal Law on Protection of Personal Data held by Private Parties. | Article 7. Personal data must be collected and processed in a lawful manner in accordance with the provisions established by this Law and other applicable regulations.<br><br>Personal data must not be obtained through deceptive or fraudulent means.<br><br>Article 12. Processing of personal data must be limited to fulfillment of the purposes set out in the privacy notice. If the data controller intends to process data for another purpose which is not compatible or analogous to the purposes set out in the privacy notice, the data owner's consent must be obtained again.<br><br>Article 13. Processing of personal data will be done as necessary, appropriate and relevant with relation to the purposes set out in the privacy notice. In particular, for sensitive personal data, the data controller must make reasonable | Articles 53, 64 y 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | efforts to limit the processing period thereof to the minimum required. | | |
| | | Regulations to the Federal Law on Protection of Personal Data held by Private Parties | Article 10. The principle of legitimacy requires the data controller to ensure that processing follows and complies with the provisions of Mexican and international law.<br><br>Article 40. Personal data may be processed only to comply with the purpose or purposes set out in the privacy notice, as provided in Article 12 of the Law.<br><br>For purposes of the previous paragraph, the purpose or purposes set out in the privacy notice shall be determined, something which will be achieved when with clarity, and without giving rise to confusion and in an objective manner, the purpose for which personal data will be processed is specified.<br><br>Article 41. The data controller shall identify and distinguish in the privacy notice between the purposes that give rise to and are necessary for the legal relationship between the data controller and the data subject from those that are not.<br><br>Article 42. The data subject may refuse or revoke his consent, as well as object to the processing of his | Articles 53, 64 y 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | personal data for purposes different from those that are necessary or that gave rise to the legal relationship between the data controller and the data subject, without this having as a consequence, the termination of the processing for the latter two purposes.<br><br>Article 45. Only personal data that are necessary, appropriate, and relevant in connection with the purposes for which they were obtained may be processed.<br><br>Article 46. The data controller must make reasonable efforts to limit the personal data processed to the minimum necessary in accordance with the purpose of the processing taking place. | | |
| | | General Law on Protection of Personal Data Held by Obligated Parties. | Article 17. The processing of personal data by the data controller must be carried out within the scope of the faculties and attributions conferred to the data controller under applicable regulations.<br><br>Article 18. All processing of personal data by the data controller must be justified as undertaken for specific, lawful, explicit and legitimate purposes relating to the attributions vested in the data controller under applicable regulations. […] | Articles 163, 164 y 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | Article 25. The data controller must process only such personal data as are suitable, relevant and strictly necessary to achieve the ends that justify their processing. | | |
| | | General Guidelines of Protection of Personal Data Held by Obligated Parties. | Articles 8, 24 and 25: i) require data controllers to process personal data in accordance with the powers established in the local legislation and with international rights, ii) define when personal data is adequate, relevant and strictly necessary for the proposes of the processing and ii) provide that the data controller shall process the minimum necessary of personal data. | Articles 163, 164 y 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |
| 4 | ***IV Use of Personal Information*** **(Ref. Para. 25)**<br>Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except:<br>a) with the consent of the individual whose personal information is collected;<br>b) when necessary to provide a service or product requested by the individual; or,<br>c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect. | Federal Law on Protection of Personal Data held by Private Parties. | Article 12. Processing of personal data must be limited to fulfillment of the purposes set out in the privacy notice. If the data controller intends to process data for another purpose which is not compatible or analogous to the purposes set out in the privacy notice, the data owner's consent must be obtained again | Articles 63, 64 y 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |
| | | Regulations to the Federal Law on Protection of Personal Data held by Private Parties | Article 40. Personal data may be processed only to comply with the purpose or purposes set out in the privacy notice, as provided in Article 12 of the Law. For purposes of the previous paragraph, the purpose or purposes set out in the privacy notice shall be determined, something which will be achieved when with | Articles 63, 64 y 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | clarity, and without giving rise to confusion and in an objective manner, the purpose for which personal data will be processed is specified.<br><br>Article 41. The data controller shall identify and distinguish in the privacy notice between the purposes that give rise to and are necessary for the legal relationship between the data controller and the data subject from those that are not.<br><br>Article 42. The data subject may refuse or revoke his consent, as well as object to the processing of his personal data for purposes different from those that are necessary or that gave rise to the legal relationship between the data controller and the data subject, without this having as a consequence, the termination of the processing for the latter two purposes.<br><br>Article 43. The data controller may not carry out processing for different purposes that are not compatible or analogous to those for which the personal data was originally collected and which were mentioned in the privacy notice unless: I. A law or regulation explicitly permits it, or II. The data controller has obtained consent for the new processing. | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | General Law on Protection of Personal Data Held by Obligated Parties. | Article 18. All processing of personal data by the data controller must be justified as undertaken for specific, lawful, explicit and legitimate purposes relating to the attributions vested in the data controller under applicable regulations.<br><br>The data controller may process personal data for purposes other than those set forth in the privacy notice, provided the data controller has the required attributions to do so as conferred by law and has obtained the data owner's consent, unless a person reported as missing is concerned, this as provided in this Law and other applicable provisions on the matter. | Articles 163, 164 y 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | |
| | | General Guidelines of Protection of Personal Data Held by Obligated Parties. | Article 9 provides that the personal data processing purpose must be concrete, explicit, legal and legitimate and describes such characteristics.<br><br>Article 10 provides the conditions for the personal data processing for secondary purposes. | Articles 163, 164 y 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |
| **5** | ***V Choice***<br>**(Ref. Para. 26)**<br>Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal | Federal Law on Protection of Personal Data held by Private Parties. | Article 8. All processing of personal data will be subject to the consent of the data owner except as otherwise provided by this Law.<br><br>Consent will be express when such is communicated verbally, in writing, by electronic or optical means or via any other technology, or by unmistakable indications.<br>It will be understood that the data | Article 63, 64 y 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | information controllers to provide these mechanisms when collecting publicly available information. | | owner tacitly consents to the processing of his data when, once the privacy notice has been made available to him, he does not express objection.<br>Financial or asset data will require the express consent of the data owner, except as provided in Articles 10 and 37 of this Law.<br>Consent may be revoked at any time without retroactive effects being attributed thereto. For revocation of consent, the data controller must, in the privacy notice, establish the mechanisms and procedures for such action.<br><br>Article 9. In the case of sensitive personal data, the data controller must obtain express written consent from the data owner for processing, through said data owner's signature, electronic signature, or any authentication mechanism established for such a purpose.<br><br>Databases containing sensitive personal data may not be created without justification of their creation for purposes that are legitimate, concrete and consistent with the explicit objectives or activities pursued by the regulated party.<br><br>Article 10. Consent for processing of personal data will not be necessary where: | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | I. Any Law so provides;<br>II. The data is contained in publicly available sources;<br>III. The personal data is subject to a prior dissociation procedure;<br>IV. It has the purpose of fulfilling obligations under a legal relationship between the data owner and the data controller;<br>V. There is an emergency situation that could potentially harm an individual in his person or property;<br>VI. It is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data owner is unable to give consent in the terms established by the General Health Law and other applicable laws, and said processing of data is carried out by a person subject to a duty of professional secrecy or an equivalent obligation, or<br>VII. A resolution is issued by a competent authority.<br><br>Article 12. Processing of personal data must be limited to fulfillment of the purposes set out in the privacy notice. If the data controller intends to process data for another purpose which is not compatible or analogous to the purposes set out in the privacy notice, the data owner's consent must be obtained again. | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | Regulations to the Federal Law on Protection of Personal Data held by Private Parties | Article 11. The data controller must obtain consent for the processing of personal data unless it is not required under Article 10 of the Law. The request for consent shall refer to a specific purpose or purposes, contemplated in the privacy notice. When personal data are obtained personally or directly from the data subject consent shall be prior to the processing.<br><br>Article 12. Obtaining consent, tacitly or explicitly, shall be: I. Free: without error, bad faith, violence or fraud that may affect the expression of the will of the data subject; II. Specific: refer to one or several specific purposes that justify the processing, and III. Informed: the data subject must previously know from the privacy notice, the processing to be done with his personal data and the consequences of granting his consent. Express consent must also be unequivocal, in other words, that there are elements that unquestionably demonstrate that it was given.<br><br>Article 13. Unless the Law requires the express consent of the data subject, tacit consent will be valid, as a general rule, pursuant to Articles 12 and 13 of these Regulations.<br><br>Article 14. When the data controller seeks to collect personal data | Article 63, 64 y 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | directly or personally from the data subject, it shall previously make available to the data subject a privacy notice which shall contain a mechanism by which, as the case may be, the data subject may state his refusal to allow the processing of his personal data for purposes different from those that are necessary and that create a legal relationship between the data controller and the data subject.<br><br>In those cases in which personal data is obtained indirectly from the data subject and cause a change in the purposes that were consented to in the transfer, the data controller shall make available to the data subject a privacy notice prior to using the personal data. When the privacy notice is not brought to the notice of the data subject directly or personally, the data subject shall have a period of five day to state, as the case may be, his refusal to allow the processing of his personal data for purposes which are different from those that are necessary and that create a legal relationship between the data controller and the data subject. If the data subject does not state his refusal to the processing of his data in accordance with the foregoing, it shall be understood that he has given his consent to the processing of the same, unless there | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | is evidence to the contrary. When the data controller uses remote or local electronic, optical or other technological means of communication mechanisms that allow personal data to be obtained automatically and simultaneously at the time the data subject has contact with the mechanisms, at the same time the data subject must be informed of the use of such technology, that through these mechanisms personal data will be obtained, and of the manner in which this can be disabled.<br><br>Article 15. The data controller must obtain the express consent of the data subject when:<br><br>I. It is required by law;<br><br>II. In the case of financial or property data;<br><br>III. In the case of sensitive data;<br><br>IV. It is requested by the data controller to prove the same, or<br><br>V. It is so agreed by the data subject and the data controller.<br><br>Article 16. When express consent is required by law, the data controller shall provide the data subject with a simple and free-of-charge means of stating this, if he so wishes.<br><br>Article 17. As provided in Articles 10(IV) and 37(VII) of the Law, tacit or | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | express consent will not be required for the processing of personal data when this arises from a legal relationship between the data subject and the data controller. The previous paragraph shall not apply when the processing of personal data is for purposes different from those that are necessary and create the legal relationship between the data controller and the data subject. In this case, to obtain tacit consent, the data controller shall observe the provisions of Article 8, third paragraph, of the Law and Articles 11, 12, and 13 of these Regulations, and with respect to sensitive, financial, or property data, it shall obtain express consent, or as required by the Law, express and written consent.<br><br>Article 18. It is considered that express consent was given verbally when the data subject gives it orally to the data controller in the latter's presence of by the use of any technology that permits oral dialogue.<br><br>Article 19. It will be considered that express consent was given in writing when the data subject provides it in a document bearing his hand-written signature, fingerprint, or any other mechanism authorized by law. In a digital environment, an electronic | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | signature may be used or any mechanism or procedure that is established for this purpose and permits the identification of the data subject and the obtaining of his consent.<br><br>Article 20. To show that consent has been obtained, the burden of proof always rests upon the data controller.<br><br>Article 21. At any time, the data subject may revoke his consent for the processing of his personal data and the data controller shall establish simple and free-of-charge mechanisms to permit the data subject to revoke his consent using at least the same media that he used to provide it, provided that the law does not prevent this. The mechanisms or procedure established by the data controller to deal with consent revocation requests may not exceed the period contemplated in Article 32 of the Law. When the data subject requests confirmation that the processing of his personal data has stopped, the data controller shall expressly respond to such request. If the personal data has been transmitted prior to the date of the revocation of consent and continue to be processed by the data processor, the data controller shall bring the | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | revocation to the attention of the data processor so that he takes the necessary steps to deal with it. | | |
| | | General Law on Protection of Personal Data Held by Obligated Parties. | Article 18. All processing of personal data by the data controller must be justified as undertaken for specific, lawful, explicit and legitimate purposes relating to the attributions vested in the data controller under applicable regulations.<br>The data controller may process personal data for purposes other than those set forth in the privacy notice, provided the data controller has the required attributions to do so as conferred by law and has obtained the data subject's consent, unless a person reported as missing is concerned, this as provided in this Law and other applicable provisions on the matter<br><br>Article 20. When any one or more of the causes for exemption contemplated in Article 22 of this Law are not present, the data controller must obtain the data owner's prior consent to process his/her personal data, which must be granted: **I.** Freely: without the involvement of error, bad faith, duress or dolus which may affect the data owner's expression of free will; **II.** Specifically: it must refer to concrete, lawful, explicit and legitimate purposes that justify their processing; and **III.** In an informed manner: the data owner being | Articles 163, 164 y 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | cognizant of the privacy notice prior to any processing of his/her personal data.<br><br>When obtaining the consent of minors or individuals whose status of interdiction or incapacity has been legally declared, the rules on representation provided for in the applicable civil laws will apply.<br><br>Article 21. Consent may be granted expressly or tacitly. Consent will be understood as expressly granted when the data owner's will has been expressed orally, in writing, by electronic or optical means, by unequivocal signs or by the use of any other technology.<br><br>Consent will be tacit when the privacy notice is made available to the data owner without him/her expressing anything to the contrary.<br><br>As a general rule tacit consent will be valid, except in the event that applicable provisions require that the data owner's will be expressly stated.<br><br>Regarding sensitive personal data, the data controller must obtain the express written consent from the data owner for its processing, by means of his/her autograph or | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | electronic signature, or by any other means of authentication established for such a purpose, except in the cases contemplated in article 22 of this Law.<br>Article 22. The data controller will not be obligated to obtain the data owner's consent to process his/her personal data in the following cases:<br><br>I. Where so provided in a statute, such assumptions having to adhere to the bases, principles and provisions set forth in this Law, without contravening it under any circumstance; II. Where transfers made between data controllers involve personal data used in exercising their own, compatible or analogous faculties for the purpose that gave rise to the processing of the personal data; III. Where there is a court order, decision or mandate grounded in law and fact issued by a competent authority;<br><br>IV. For the recognition or defense of the data owner's rights before a competent authority; V. Where the personal data are required to exercise a right or comply with obligations arising from a legal relationship between the data owner and the data controller; VI. Where an emergency arises that has the potential of causing damage or injury to the person or property of an | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | individual; VII. Where the personal data are required to provide preventive treatment or diagnosis when providing healthcare; VIII. Where the personal data are contained in public access sources; IX. Where the personal data have been subject to a prior dissociation process; or X. Where the data owner is a person reported as missing as provided in the law on the matter. | | |
| | | General Guidelines of Protection of Personal Data Held by Obligated Parties. | Articles 12 to 20, which provide specifications on how to obtain consent, modalities of consent and when to apply them, as well as how to revoke consent. | Articles 163, 164 y 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |
| **6** | ***VI Integrity of Personal Information*** **(Ref. Para. 27)** Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use. | Federal Law on Protection of Personal Data held by Private Parties. | Article 11. The data controller shall ensure that personal data contained in databases is relevant, correct and up-to-date for the purposes for which it has been collected. When the personal data is no longer necessary for the fulfillment of the objectives set forth in the privacy notice and applicable law, it must be cancelled. The controller of the database will be required to remove information relating to nonperformance of contractual obligations, after a period of seventy-two months counted from the calendar day on which said nonperformance arose. | Articles 63, 64 y 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | Regulations to the Federal Law on Protection of Personal Data held by Private Parties | Article 36. The personal data processed by the data controller will meet the principle of quality when they are exact, complete, pertinent, correct, and up-to-date as required to comply with the purpose for which they are processed. Personal data are presumed to comply with quality when they are directly provided by the data subject until he declares and proves otherwise, or the data controller has objective evidence contradicting this. When the personal data were not obtained directly from the data subject, the data controller must take reasonable measures for it to meet the principle of quality in accordance with the type of personal data and the processing conditions. The data controller must adopt the mechanisms that it considers necessary to ensure that personal data dealt with are exact, complete, pertinent, correct, and up-to-date so that the truth of the data are not altered and the data subject thereby prejudiced by this.<br><br>Article 37. The preservation periods for personal data may not exceed those necessary to achieve the purposes that justify the processing and shall comply with the law applicable to the subject matter involved and take into account the administrative, accounting, tax, legal, and historical aspects of the information. After the purpose or purposes of processing have been | Articles 63, 64 y 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | achieved, the data controller must cancel the data in its collection after blocking them for subsequent suppression.<br><br>Article 38. Data controllers must establish and document procedures for the preservation, and if necessary, blockage and suppression of personal data, including periods of preservation thereof, in accordance with the previous Article.<br><br>Article 39. The data controller must show that personal data is preserved, or if applicable, blocked, suppressed, or cancelled in accordance with the periods set out in Article 37 of these Regulations or taking into account a request of the right to cancelation. | | |
| | | General Law on Protection of Personal Data Held by Obligated Parties. | Article 23. The data controller must take the necessary measures to maintain the accuracy, completeness, and correctness of the personal data held by it and to keep them up to date, so as not to alter their veracity.<br><br>There is the presumption that quality of personal data has been complied with when the same have been directly provided by the data owner, unless and until otherwise expressed and evidenced by the data owner. | Article 163, 164 y 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | Where personal data are no longer needed to achieve the purposes specified in the privacy notice which gave rise to their processing in accordance with applicable provisions, they must be suppressed, having first been blocked if required, once the term provided for their preservation has elapsed.<br><br>The terms for preservation of personal data must not exceed those that are necessary to achieve the purposes that warranted their processing, must adhere to the applicable provisions on the relevant matter and take into consideration the administrative, accounting, tax, legal and historical aspects of the personal data.<br><br>Article 24**.** The data controller must establish and document the procedures to be followed for preservation and, such being the case, blocking and suppression of personal data, which must specify the terms for preservation of the same, in accordance with the provisions of the preceding article of this Law.<br><br>In the procedures mentioned in the preceding paragraph, the data controller must include mechanisms | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | that allow for compliance with the terms established for the suppression of personal data, as well as for conducting periodic review on the need for preserving the personal data. | | |
| | | General Guidelines of Protection of Personal Data Held by Obligated Parties. | Articles 21, 22 y 23, which provide the definitions of correct, complete and up dated personal data; the obligation of the data controller to adopt measures to assure personal data quality when not obtained directly from the data subject; and the policies, methods and techniques that must be put in place for the personal data deletion. | Articles 163, 164 y 165 of the General Law on Protection of Personal Data Held by Obligated Parties | Enacted |
| **7** | ***VII Security Safeguards*** **(Ref. Para. 28)** Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. | Federal Law on Protection of Personal Data held by Private Parties. | Article 19. All responsible parties that process personal data must establish and maintain physical and technical administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing.<br><br>Data controllers will not adopt security measures inferior to those they keep to manage their own information. Moreover, risk involved, potential consequences for the data owners, sensitivity of the data, and technological development will be taken into account.<br><br>Article 20. Security breaches occurring at any stage of processing | Article 58 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties: Pursuant to Article 65 (III) of the Law, whenever there is a breach of personal data security, the Institute may take into consideration compliance with its recommendations in determining a reduction in a penalty.<br><br>…and articles 63, 64 y 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | that materially affect the property or moral rights of data owners will be reported immediately by the data controller to the data owner, so that the latter can take appropriate action to defend its rights.<br><br>Article 21. The data controller or third parties involved in any stage of personal data processing must maintain confidentiality with respect to such data, and this obligation will continue even after the end of its/their relationship with the data owner or, as the case may be, with the data controller. | | |
| | | Regulations to the Federal Law on Protection of Personal Data held by Private Parties | Article 57. The data controller, and as applicable, the data processor, must establish and maintain administrative, physical, and if applicable technical, security measures for the protection of personal data pursuant to the Law and this Chapter, regardless of the processing system. For the purposes of this Chapter, security measures mean security control or group of controls to protect personal data. The above is without prejudice to the laws and regulations in force with respect to security issued by the competent authorities in the corresponding sector when they contemplate greater protection for data subjects than that provided in the Law and these Regulations. | Article 58 of the Regulations to the Federal Law on Protection of Personal Data held by Private Parties: Pursuant to Article 65 (III) of the Law, whenever there is a breach of personal data security, the Institute may take into consideration compliance with its recommendations in determining a reduction in a penalty.<br><br>…and articles 63, 64 y 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | Article 59. To establish and ensure effective security measures, the data controller may take its own security measures or may contract these to an individual or corporate body.<br><br>Article 60. The data controller shall determine the security measures applicable to personal data, taking into account the following factors:<br><br>I. The inherent risk by type of personal data;<br><br>II. The sensitivity of the personal data processed;<br><br>III. Technological development, and<br><br>IV. The possible consequences of a violation for the data subjects. In addition, the data controller shall try to take the following factors into account:<br><br>I. The number of data subjects;<br><br>II. The vulnerabilities previously encountered in the processing systems;<br><br>III. The risk as a result of the potential quantitative or qualitative value that the personal data may have to an unauthorized third party having possession of the data, and<br><br>IV. Other factors that may have an impact upon the level of risk or which | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | result from other laws or regulations applicable to the data controller.<br><br>Article 61. In order to establish and maintain the security of personal data, the data controller must take into account the following actions<br><br>I. Prepare an inventory of personal data and processing systems;<br><br>II. Determine the duties and obligations of those who process personal data;<br><br>III. Have a risk analysis of personal data consisting of identifying dangers and estimating the risks to the personal data;<br><br>IV. Establish the security measures applicable to personal data and identify those implemented effectively;<br><br>V. Analyze the gap between existing security measures and those missing that are necessary for the protection of personal data;<br><br>VI. Prepare a work plan for the implementation of the missing security measures arising from the gap analysis;<br><br>VII. Carry out reviews and audits; | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | VIII. Train personnel who process personal data, and<br><br>IX. Keep a record of personal data storage media. The data controller shall prepare a document setting out security measures arising from the previous paragraphs.<br><br>Article 62. Data controllers must update the document setting out security measures when the following events occur:<br><br>I. Modifications to the security measures or processes are made for their continuous improvement, arising from revisions of the security policy of the data controller;<br><br>II. Substantial modifications are made in the processing arising from a change in the level of risk;<br><br>III. Processing systems are violated, as provided in Article 20 of the Law and Article 63 of these Regulations, or<br><br>IV. There is an impact upon the personal data other than the above. In the case of sensitive personal data, the data controller shall review, and if necessary update the security document once a year. | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | Article 63. Breaches of the security of personal data which occur in each processing phase are:<br><br>I. Loss or unauthorized destruction;<br><br>II. Theft, misplacement or unauthorized copying;<br><br>III. Unauthorized use, access or processing, or<br><br>IV. Unauthorized damage, alteration or modification.<br><br>Article 64. The data controller must inform the data subject, without delay, of breaches that significantly prejudice the property or nonpecuniary rights of the data subjects upon confirming the breach and having taken action to trigger an exhaustive review of the magnitude of the breach so that the prejudiced data subjects may take the appropriate measures.<br><br>Article 65. The data controller must inform the data subject of at least the following:<br><br>I. The nature of the breach;<br><br>II. The personal data compromised;<br><br>III. Recommendations to the data subject concerning measures that | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | the latter can adopt to protect his interests;<br><br>IV. Corrective actions implemented immediately, and<br><br>V. The means by which he may obtain more information in this regard.<br><br>Article 66. In case of a breach of the personal data, the data controller must analyze the causes of its occurrence and implement the corrective, preventive and improvement steps to make the security measures adequate in order to avoid a repetition of the breach. | | |
| | | General Law on Protection of Personal Data Held by Obligated Parties. | Article 31. Regardless of the type of system on which personal data are hosted or the type of processing applied, the data controller must establish administrative, physical and technical security measures to protect personal data that afford protection against damage, loss, alteration, destruction or unauthorized use, access to, or processing, and must ensure their confidentiality, integrity and availability.<br><br>Article 32. The security measures adopted by the data controller must | Articles 163, 164 y 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | take into consideration: **I.** The inherent risk regarding processed personal data; **II.** The sensitivity of the processed personal data; **III.** Technological developments; **IV.** The possible consequences of a breach affecting data owners; **V.** The personal data transfers to be made; **VI.** The number of data owners; **VII.** The previous breaches that have occurred in the processing systems; and **VIII. T**he risk relating to the potential quantitative or qualitative value processed personal data may have for a third party lacking authorization to hold them.<br><br>Article 33. In establishing and maintaining the security measures required for personal data protection, the data controller must undertake, at the least, the following interrelated activities: **I.** Establishing internal policies on personal data management and processing that take into account the context in which processing is to take place and the personal data lifecycle, that is to say, their collection, use and ulterior suppression; **II.** Defining the functions and obligations of the personnel involved in the processing of the personal data; **III.** Taking an inventory of the personal data and of the processing systems; **IV.** Conducting risk analysis on the | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | personal data, taking into account existing threats and vulnerabilities regarding the personal data and the resources involved in their processing; such as the hardware, software, the data controller's personnel, among others, these listed here as an enumeration and not by way of limitation; **V.** Performing gap analysis by comparing existing security measures against those still lacking in the data controller's organization; **VI. P**reparing a work plan for the implementation of the security measures found lacking, as well as for the implementation of measures for daily compliance with the personal data management and processing policies, **VII.** Monitoring and reviewing implemented security measures, as well as the threats and vulnerabilities to the personal data from time to time; and **VIII.** Designing and applying different training levels for personnel under its command, depending on their roles and responsibilities in regard to the processing of personal data.<br><br>Article 34. The actions relating to the personal data processing security measures must be documented and kept in a management system.<br><br>A management system will be understood to be the set of | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | interrelated elements and activities set up to establish, implement, operate, monitor, review, maintain and improve the processing and security of personal data, in accordance with the provisions of this Law and other applicable provisions on the matter.<br><br>Article 35. In particular, the data controller must prepare a security document containing, at least, the following: **I.** The inventory on the personal data and the processing systems; **II.** The functions and duties of the persons involved in the processing of personal data; **III.** Risk analysis; **IV.** Gap analysis; **V.** Work plan; **VI.** The monitoring and review mechanisms regarding security measures; and **VII.** The general training program.<br><br>Article 36. The data controller must update the security document whenever any of the following events occurs: **I.** Substantial changes in the processing of the personal data are made that entail a change in risk level; **II.** As a result of a continuing improvement process, arising from the monitoring and review of the management system; **III.** As a result of an improvement process intended | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | to mitigate the impact of a security breach that may have occurred; and **IV.** After the implementation of corrective and preventive measures as a result of a security breach.<br><br>Article 37. Should a security breach occur, the data controller must analyze the causes that gave rise to it and include in its work plan the preventive and corrective actions required to adapt the security measures and the personal data processing, such being the case, so as to prevent the breach from occurring again.<br><br>Article 38. In addition to those specified in the relevant laws and in applicable regulations, any of the following events, listed here as a minimum, are considered to be security breaches at any phase in the processing of personal data: **I.** Loss or unauthorized destruction; **II.** Theft, misplacement or unauthorized copying; **III.** Unauthorized use, access or processing; and **V.** Damage to and unauthorized alteration or modification. | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | Article 39. The data controller must keep a logbook to record security breaches, which must include a description of same, date of occurrence, their causes and the corrective measures that were implemented forthwith and definitively.<br><br>Article 40. The data controller must forthwith inform the data owner and, as applicable, the Institute and the Guarantor bodies of the Federated States, on any breaches that significantly affect economic or moral rights, upon confirmation that a breach has occurred, and once the data controller has begun to take the action required to trigger in-depth examination in regard to the extent of the breach, so as to enable affected data owners to take the required measures to defend their rights.<br><br>Article 41. The data controller must provide the data owner with at least the following information: **I.** The nature of the incident; **II.** The compromised personal data; **III.** Recommendations to the data owner on the measures he/she may adopt to protect his/her own interests; **IV.** The corrective actions that were | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | implemented forthwith; **V.** The media where more information on the matter may be obtained.<br><br>Article 42. The data controller must establish controls or mechanisms intended to ensure that any and all persons involved in any phase of the processing of personal data maintain the confidentiality of the same. This obligation must survive termination of their relationship with the data controller.<br><br>The foregoing without prejudice to the provisions regarding access to public information. | | |
| | | General Guidelines of Protection of Personal Data Held by Obligated Parties. | Articles 55 to 72, which provide the obligation of the data controller to maintain security measures; including internal policies of personal data management; the establishment of roles and responsibilities of staff processing personal data; to develop a personal data inventory and processes related to the personal data held by them; development of risk and gap analysis; working plan and periodical monitoring mechanisms of the security measures put in place by the data controller and training procedures. | Articles 163, 164 y 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | These articles also provide terms to notify authorities and data subjects any data breaches occurred and actions from the national data authority derived from these notifications, including the issuance of recommendations.<br><br>As well as the controller's obligation to establish controls or mechanisms intended to all the people involved at any phase of the processing of personal data to keep confidentiality. | | |
| **8** | ***VIII Access and Correction*** **(Ref. Para. 29-31)**<br>Individuals should be able to:<br>a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;<br>b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;<br>i. within a reasonable time;<br>ii. at a charge, if any, that is not excessive;<br>iii. in a reasonable manner;<br>iv. in a form that is generally understandable; and,<br>c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted. | Federal Law on Protection of Personal Data held by Private Parties. | Article 22. Any data owner, or, where appropriate, his legal representative, may exercise the rights of access, rectification, cancellation and objection under this Law. The exercise of any of these is not a prerequisite nor does it impede the exercise of another. Personal data must be preserved in such a way as to allow the exercise of these rights without delay.<br><br>Article 23. Data owners will have the right to access their personal data held by the data controller as well as to be informed of the privacy notice to which processing is subject.<br><br>Article 24. The data owner will have the right to rectify data if it is inaccurate or incomplete.<br><br>Article 28. The data owner or his legal representative may at any time | Articles 63, 64 y 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | Such access and opportunity for correction should be provided except where:<br>(i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question;<br>(ii) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or<br>(iii) the information privacy of persons other than the individual would be violated.<br>If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial. | | make a request to the data controller for access, rectification, cancellation or objection in relation to the personal data concerning him.<br><br>Article 29. The access, rectification, cancellation or objection request must include the following:<br><br>I. The data owner's name and address or other means to notify him of the response to his request;<br><br>II. Documents establishing the identity or, where appropriate, legal representation of the data owner;<br><br>III. A clear and precise description of the personal data with regard to which the data owner seeks to exercise any of the abovementioned rights.<br><br>IV. Any other item or document that facilitates locating the personal data.<br><br>Article 30. All data controllers must designate a personal data person or department who will process requests from data owners for the exercise of the rights referred to in this Law. In addition, data controllers will promote protection of personal data within their organizations. | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | Article 31. In the case of requests for rectification of personal data, the data owner must indicate, in addition to that which is specified in the preceding article of this Law, the changes to be made, and provide documentation supporting the request.<br><br>Article 32. The data controller will notify the data owner, within a maximum of twenty days counted from the date of receipt of the request for access, rectification, cancellation or objection, of the determination made, so that, where appropriate, same will become effective within fifteen days from the date on which the notice is provided. For personal data access requests, delivery will be made upon proof of identity of the requesting party or legal representative.<br><br>The aforementioned time periods may be extended a single time by a period of equal length, provided that such action is justified by the circumstances of the case.<br><br>Article 33. The obligation to provide access to information will be fulfilled when the personal data is made available to the data owner; or, by issuing uncertified copies, electronic documents or any other means | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | established by the data controller in the privacy notice.<br><br>In the event that the data owner requests access to data from a person or entity who he presumes is the data controller and said person or entity proves not to be such, it will be sufficient for said person or entity to so indicate to the data owner by any of the means referred to in the preceding paragraph, for the request to be considered properly fulfilled.<br><br>Article 34. The data controller may deny access to personal data or refuse the rectification, cancellation or objection with relation thereto in the following cases:<br><br>I. Where the requesting party is not the subject of the personal data, or the legal representative is not duly accredited for such purposes;<br><br>II. Where the requesting party's personal data is not found in the data controller's database;<br><br>III. Where the rights of a third party are adversely affected;<br><br>IV. Where there is any legal impediment, or decision of a competent authority, restricting | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | access to the personal data or not allowing the rectification, cancellation or objection with relation thereto, and<br><br>V. Where the rectification, cancellation or objection has been previously performed?<br><br>The refusal referred to in this article may be partial, in which case the data controller will carry out the access, rectification, cancellation or objection requested by the data owner.<br><br>In all of the aforementioned cases, the data controller must notify the data owner, or, as appropriate, his legal representative, of its decision and the reason for such decision, within the periods established for such purposes, via the same means by which the request was made, attaching, where appropriate, any relevant evidence.<br><br>Article 35. The action of providing personal data will be free, and the data owner must only pay justified expenses of shipping or the cost of copying or providing data in other formats.<br><br>This right will be exercised by the data owner free of charge, upon proof of his identity to the data | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | controller. However, if the same person repeats his request within a period of twelve months, costs will not be greater than three days of the General Current Minimum Wage in Mexico City, unless there are material changes to the privacy notice that prompt new queries.<br><br>The data owner may file a data protection request due to the response received or lack of response from the data controller, in accordance with the provisions of the following Chapter. | | |
| | | Regulations to the Federal Law on Protection of Personal Data held by Private Parties | Article 87. The exercise of any of the ARCO rights does not exclude the possibility of exercising another of them nor of this being a requirement to be fulfilled prior to exercising any of these rights.<br><br>Article 88. The exercise of ARCO rights may be restricted for reasons of national security, by laws and regulations of a public policy nature, for reasons of public health and safety, or to protect the rights of third parties in those cases and to the extent contemplated in the laws applicable to the matter, or by a decision of a competent authority well-founded in law and fact.<br><br>Article 89. ARCO rights may be exercised:<br>I. By the data subject, after proving | Articles 63, 64 y 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | his identity through the presentation of a copy of his identity document and having shown the original for comparison. Also admissible will be the electronic instruments by which it is possible to reliably identify the data subject and other authentication mechanisms permitted by law or previously established by the data controller. The use of an advanced electronic signature or the electronic instrument replacing it will exempt the data subject from the need to present a copy of the identification document, and<br>II. By the representative of the data subject, after proving:<br>a) the identity of the data subject;<br>b) the identity of the representative, and<br>c) the existence of the representation by means of a public instrument or simple power of attorney signed before two witnesses or by personal attendance by the data subject. For the exercise of ARCO rights by minors or by a person under interdiction or without legal capacity, the representation rules of the Federal Civil Code shall apply.<br><br>Article 90. For the exercise of ARCO rights, the data subject may submit, personally or through a representative, a request to the data controller using the means established in the privacy notice. For such purpose, the data controller shall make available to the data | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | subject remote or local electronic communication means or such others as it considers appropriate. In addition, the data controller may establish forms, systems, and other simplified methods to help data subjects exercise the ARCO rights and these must be mentioned in the privacy notice.<br><br>Article 91. When the data controller has customer service of any type or services for the resolution of claims related to the service rendered or the products offered, the data controller may resolve requests for the exercise of ARCO rights through such services, provided that the periods do not contradict those set out in Article 32 of the Law. In this case, the identity of the data subject is deemed proven by the means established by the data controller for the identification of the data subjects in providing its services or contracting for its products, provided that such means guarantee the identity of the data subject.<br><br>Article 92. When the law applicable to certain databases or processing establishes a specific procedure for requesting the exercise of ARCO rights, the provisions that offer the better guarantees to the data subject and that do not contradict the provisions of the Law, shall apply.<br><br>Article 93. The exercise of ARCO | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | rights shall be simple and free-of-charge and the data subject need only pay expenses for shipping, reproduction, and if applicable, certification of documents, with the exception provided in Article 35, second paragraph, of the Law. The costs of reproduction may not be higher than the costs of recovery of the corresponding material. The data controller may not establish, as the only way to present requests to exercise ARCO rights, any service or means with a cost.<br><br>Article 94. For the purposes of Article 29 (I) of the Law, the request for access must show an address or some other means for notification of the response to the request. If this requirement is not complied with, the data controller shall deem the request not presented, and note this for the record.<br><br>Article 95. The data controller must process any request for the exercise of ARCO rights. The period to resolve the request will be calculated from the day it was received by the data controller and it will record the latter on the acknowledgement of receipt given to the data subject. The period stated shall be interrupted if the data controller requires information from the data subject, as provided in the following Article.<br><br>Article 96. If the information provided | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | in the request is insufficient or inaccurate and so cannot be dealt with, or if the documents referred to in Articles 29 (II) and 31 of the Law are not attached, the data controller may ask the data subject once, within five days after receipt of the request, to provide the items or documents necessary for its processing. The data subject shall have ten days to attend to the request, calculated from the day following the date on which it was received. If no response is provided within this period, the request will be considered as not having been submitted. If the data subject attends to the request for information, the period that the data controller has to respond to the request begins to run from the day following that on which the data subject attends to the request. If the data controller does not request additional documentation from the data subject to prove his identity or the legal status of his representative, the same shall be considered as proven by the documentation provided by the data subject in his request.<br><br>Article 97. Pursuant to Article 32, second paragraph of the Law, if the data controller decides to extend the period to respond a request for the exercise of ARCO rights or the period for implementing the response, it must notify the applicant of the justification for the extension, | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | within either of the following periods:<br>I. In the case of an extension of twenty days to communicate the decision adopted on the admissibility of the request, the justification for the extension must be communicated within the same period, calculated from the date the request is received, or<br>II. In the case of an extension of fifteen days to enforce the right in question, the justification of the extension must be communicated within the same period, calculated from the date of the notification of the admissibility of the request.<br><br>Article 98. In all cases, the data controller must respond the request for the exercise of ARCO rights that it receives, regardless of whether or not the personal data of the data subject appear in its databases, within the periods established in Article 32 of the Law. The response from the data controller shall only refer to the personal data that have been specifically mentioned in the request and must be presented in a legible and understandable format with easy access. In case of the use of codes, initials, or keys, the corresponding meanings must be provided.<br><br>Article 99. When access to the personal data is on site, the data controller must determine the period during which the data subject may | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | come to consult them, which may not be less than fifteen days. If this period lapses and the data subject has not come to obtain access to his personal data, it will be necessary to submit a new request.<br><br>Article 100. A data controller must justify its refusal to grant the exercise of ARCO rights and inform the data subject of his right to request the commencement of proceedings for the protection of rights with the Institute.<br><br>Article 101. Pursuant to Article 23 of the Law, the data subject has the right to obtain his personal data from the data controller, as well as information regarding the conditions and general features of the processing.<br><br>Article 102. The obligation to give access will be considered as complied with when the data controller makes available to the data subject personal data on site, respecting the period set out in Article 99 of these Regulations, or by issuing photocopies or using magnetic, optical, sound, visual, or holographic media, as well as other information technologies contemplated in the privacy notice. In all cases access must be granted in formats which are readable and comprehensive to the data subject. When the data controller considers it | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | appropriate, it may agree with the data subject upon reproduction media for the information different from that mentioned in the privacy notice.<br><br>Article 103. Pursuant to Article 24 of the Law, the data subject may request, at any time, from the data controller, a rectification or correction of his personal data that are inaccurate or incomplete.<br><br>Article 104. The request for rectification must indicate to what personal data it refers, as well as the rectification or correction to be made, and must be accompanied by the documentation proving the admissibility of the request. The data controller may offer mechanisms for the benefit of the data subject to facilitate the exercise of this right.<br><br>Article 105. Pursuant to Article 25 of the Law, cancellation means stopping the processing of personal data by the data controller, starting from their blockage and subsequent suppression.<br><br>Article 106. The data subject may request, at any time, that the data controller cancel the personal data when he considers that they are not being processed in accordance with the principles and duties established by the Law and these Regulations. | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | The cancellation shall proceed with respect to all personal data of the data subject contained in a database, or only part thereof, as requested.<br><br>Article 107. If the cancellation is warranted, and without prejudice to the provisions of Article 32 of the Law, the data controller shall: I. Establish a blockage period only for the purpose of determining possible liability with respect to the processing, up to the legal or contractual limitation period, and so notify the data subject or his representative in the reply to the request for cancellation to be issued within the period of twenty days set out in Article 32 of the Law; II. Take appropriate security measures for the blockage; III. Put the blockage into effect within the period of fifteen days set out in Article 32 of the Law, and IV. After the blockage period, carry out the suppression using the security measures previously established by the data controller.<br><br>Article 108. Pursuant to Article 3 (III) of the Law, the blockage has as its purpose the prevention of processing, with the exception of storage, or possible access by any person, unless otherwise established by law. The blockage period will be until the limitation period or contractual period. | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | Article 109. Pursuant to Article 27 of the Law, the data subject may, at any time, object to the processing of his personal data or require it to stop when: I. There is a legitimate reason for doing so and his specific situation so requires, in which case, he must justify the fact that, even though the processing is lawful, it must stop in order to avoid its continuation causing prejudice to the data subject, or II. He needs to state his objection to the processing of his personal data in order to avoid processing for specific purposes.<br>The exercise of the right to object may not be exercised in those cases where the processing is necessary to comply with a legal obligation imposed on the data controller. | | |
| | | General Law on Protection of Personal Data Held by Obligated Parties. | Article 43. The data owner or his/her representative may at any time request the data controller access to, rectification or cancelation of his/her personal data, or express his/her opposition to their processing, as set forth in this Title. The exercise of any one of the ARCO rights does not constitute a prior requirement for, nor does it preclude the exercise of any other of these rights.<br><br>Article 44. The data owner will be entitled to access his/her personal | Article 163, 164 y 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | data held by the data controller, as well as to know the information regarding the conditions and general characteristics of its processing.<br><br>Article 45. The data owner will be entitled to request the data controller to rectify or correct his/her personal data when these are inaccurate, incomplete or are not updated.<br><br>Article 48. The reception and processing of requests to exercise ARCO rights submitted to data controllers will be subject to the procedure set forth in this Title and other applicable provisions on the matter.<br><br>Article 49. In order to exercise ARCO rights, the data owner must provide proof of identity, and in addition proof of identity and legal capacity of his/her representative, such being the case.<br>ARCO rights may be exercised exceptionally by a person other than the data owner or his/her representative, in the events contemplated in legal provisions, or else, under court order.<br>The exercise of ARCO rights of minors or individuals whose status of interdiction or incapacity has been legally declared under civil law, will | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | be subject to the rules for representation set forth in such legislation.<br>In regard to personal data of the deceased, the person that provides proof of legal interest in accordance with applicable laws may exercise the rights granted by this Chapter, provided the data owner should have unquestionably stated his will on this matter or there is a court order to this effect.<br><br>Article 50. The exercise of ARCO rights must be free of charge. Fees may be charged solely to recover the cost of copying, certification or delivery services as provided in applicable regulations.<br><br>In regard to access to personal data, the laws establishing copying and certification fees must take into consideration that the amounts determined should allow or facilitate the exercise of this right.<br><br>When the data owner provides the magnetic or electronic medium or the mechanism required to make copies of his/her personal data, the same must be delivered to him/her free of charge.<br><br>The information must be delivered free of charge when the delivery of | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | no more than twenty pages is involved. Transparency units may release the data owner from payment of copying and delivery fees taking into account the data owner's social and financial circumstances.<br><br>The data controller cannot condition the filing of requests to exercise ARCO rights to the use of any service o means that entails a cost for the data owner.<br><br>Article 51. The data controller must establish simple procedures to allow the exercise of ARCO rights, whose time of response should not exceed twenty days counted as of the day following reception of the request.<br><br>The term referred to in the preceding paragraph may be extended once up to ten days if so warranted by the circumstances, provided the data owner is so informed within the term provided for response.<br><br>Should the exercise of ARCO rights be found warranted, the data controller must enable such exercise within a term that cannot exceed fifteen days counted as of the day following that on which the response is notified to the data owner. | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | Article 52. Requests to exercise ARCO rights cannot be subject to requirements other than the following: **I.** The specification of the data owner's name and address or other means to receive notification; **II.** The documents providing proof of the data owner's identity and, such being the case, of the identity and legal capacity of his/her representative; **III.** If possible, specification of the area in charge of processing the personal data, and the entity before whom the request is filed; **IV.** A clear and accurate description of the personal data in regard to which the exercise of any of the ARCO rights is being sought, unless the right to access is involved; **V.** The description of the ARCO right to be exercised; or else, of that which is being requested by the data owner; and **VI.** Any other element or document that facilitates tracing of the personal data, such being the case.<br><br>Regarding a request for access to personal data, the data owner must specify the preferred form to be used in their reproduction. In processing the request, the data controller must honor the data owner's preference unless there is a physical or legal obstacle preventing it from | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | reproducing the personal data in the form requested. In such event, it must offer other forms of delivery of the personal data and must specify the legal and factual grounds for doing so.<br><br>In the event a request for the protection of the data does not meet any one of the requirements referred to in this article, and the Institute or the Guarantor bodies do not have the means to supply for its deficiencies, the data owner will be so notified once, within five days following the date the request for the exercise of ARCO rights was filed, to allow him/her to cure any deficiencies within a term of ten days counted as of the day following such notification.<br><br>Should this term elapse without the action as requested having been taken, the request to exercise ARCO rights will be deemed as not having been filed.<br><br>The notice will have the effect of staying the term the Institute, or such being the case the Guarantor bodies; have to resolve on the request for the exercise of ARCO rights.<br>In regard to a request for c cancellation, the data owner must specify the reasons for requesting the suppression of his/her data from | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | the data controller's files, records or databases.<br><br>With respect to a request expressing opposition, the data owner must specify the legitimate causes or the specific circumstances that give rise to his/her opposition to processing, and the damage or injury continued processing would cause, or if such were the case, the specific purposes for which he/she wishes to exercise the right to opposition.<br><br>Requests for the exercise of ARCO rights must be filed with the data controller´s Transparency Unit considered appropriate by the data owner, by submitting a brief, in the forms, electronic or any other media as are established by the Institute and the Guarantor bodies within the scope of their respective purviews.<br><br>The data controller must process all requests submitted for the exercise of ARCO rights and properly acknowledge receipt thereof.<br><br>The Institute and the Guarantor bodies may, as applicable, establish the forms, systems and other simplified methods required to facilitate the exercise of ARCO rights for data owners. | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | The means and procedures put in place by the data controller to handle the requests submitted for the exercise of ARCO rights must be easily accessible and provide the widest coverage, taking into account the data owners' profiles and the manner in which they maintain daily or regular contact with the data controller.<br><br>Article 53. In the event the data controller is not the appropriate entity to process the request for the exercise of ARCO rights, it must so inform the data owner within three days following submission of the request, and if capable of making the determination as to the appropriate data controller, it must refer the data owner to the latter.<br><br>In the event the data controller states that the personal data are not found in its archives, records, systems or on file, this statement must be set down in a resolution issued by the Transparency Committee confirming the non-existence of the personal data.<br><br>In the event the data controller becomes aware that the request for the exercise of ARCO rights is being filed in regard to rights not contemplated in this Law, it must so | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | inform the data owner and refer him/her to the proper authorities.<br><br>Article 54. Where the provisions applicable to certain personal data processing contemplate a specific handling or procedure to request exercise of ARCO rights, the data controller must inform the data owner on the existence of such requirement, within a term not to exceed five days following the date the request is filed, so as to allow the data owner to decide whether he/she is to exercise his/her rights resorting to such specific procedure, or else, will resort to the institutional procedure set up by the data controller to handle requests for the exercise of ARCO rights in accordance with the provisions of this Chapter.<br><br>Article 55. The only instances in which the exercise of ARCO rights will be found not to be warranted are listed herein below: **I.** Should the data owner or his/her representative not provide evidence of their legal capacity to do so; **II.** Should the personal data not be held by the data controller; **III.** Should there be a legal impediment; IV**.** Should the infringement of rights of a third party be involved; **V.** Should such exercise | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | operate to obstruct judicial or administrative proceedings; **VI.** Should there exist a resolution by a competent authority that restricts access to the personal data, or prevents rectification or cancellation of, or opposition to the same; **VII.** Should cancellation or opposition rights have already been exercised; **VIII.** Should the data controller not be the competent authority; **IX.** Should it be necessary to protect the data owner's legally protected interests; **X.** Should it be necessary in order to comply with legally acquired obligations binding upon the data owner; **XI.** Should the Mexican State, acting on the basis of its legal attributions, find that it is required and proportional to make daily use, keep and handle [personal data] in order to preserve the integrity, stability and permanence of the Mexican State; or **XII.** Should the personal data be part of information that the entities subject to financial regulation and oversight by the obligated party have provided the latter in order to comply with demands for information on their operations, organization and activities.<br><br>In all the foregoing instances, the data controller must inform the data owner on the reasons for its determination, within the term of twenty days referred to in the first paragraph of article 51 of this Law | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | and other applicable provisions, and must do so through the same means through which the request was filed, attaching any pertinent evidence, if so required.<br><br>Article 56. The petition for review referred to in article 94 of this Law is available in the event the data controller refuses to process any request for the exercise of ARCO rights or fails to provide an answer to such request.<br><br>Article 57. Where personal data are processed via electronic means in a commonly used structured format, the data owner will be entitled to obtain from the data controller a copy of the processed data in a commonly used structured electronic format allowing him/her their continuous use.<br><br>Where the data owner has provided personal data and processing is based on consent or contract, he/she will be entitled to transmit such personal data and any other information he/she may have provided, which is kept in an automated processing system, to another system in a commonly used electronic format, no impediment being placed by the processing data | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | controller that is being subjected to removal of the personal data.<br><br>The National System will establish guidelines providing for the parameters to be taken into consideration to determine the hypotheses under which the presence of a commonly used structured format is presumed to be present, as well as for the technical standards, modalities and procedures for the transfer of personal data. | | |
| | | General Guidelines of Protection of Personal Data Held by Obligated Parties. | Article 73 provides who can request the exercise of ARCO rights.<br><br>Articles 74 and 75 defines how to exercise ARCO rights of minors, persons with disabilities and regarding diseased persons.<br><br>Articles 76 to 82 specify the mechanisms for the accreditation of the identity of data subjects, representatives, minors, persons with disabilities and diseased.<br><br>Articles 83 to 91 define the elements to request the exercise of any ARCO right; assistance form the Transparency Unit; the duty of data controller to deliver data subject notice upon receipt of his request; the possibility to ask to more information from the data subject if need and specific aspects of the | Article 163, 164 y 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | procedure to address the data subject request.<br><br>Articles 92 to 95 describe how data controllers may address the request to exercise any ARCO right.<br><br>Articles 96 to 98 describe how to deliver requested personal data to the data subject by certified mail and electronic means. They also require the data controller to make the personal data or evidence related to the exercise of any specific right available for a period of 60 days.<br><br>Articles 99 to 102 describe when a request of the exercise of any ARCO right may be denied by the data controller.<br><br>Articles 103 to 106 establish some principles regarding specific proceedings provided by data controllers in order for data subjects to exercise their ARCO rights.<br><br>Article 106 provides the possibility for the data subject to file before the national data protection authority a petition of review for any disagreement related to the exercise of his ARCO rights. | | |
| **9** | ***IX Accountability*** **(Ref. Para. 32)** A personal information controller should be accountable for complying with measures that | Federal Law on Protection of Personal Data held by Private Parties. | Article 6. Data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the Law. | Articles 63, 64 and 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | give effect to the Principles stated above.<br>When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles. | | Article 14. - The data controller shall ensure compliance with the personal data protection principles established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller. The data controller must take all necessary and sufficient action to ensure that the privacy notice given to the data owner is respected at all times by it or by any other parties with which it has any legal relationship.<br><br>Article 36. Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his data; moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data.<br><br>Article 37. Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases: | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | I. Where the transfer is pursuant to a Law or Treaty to which Mexico is party;<br>II. Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management;<br>III. Where the transfer is made to holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies;<br>IV. Where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party;<br>V. Where the transfer is necessary or legally required to safeguard public interest or for the administration of justice;<br>VI. Where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and VII. Where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data owner. | | |
| | | Regulations to the Federal Law on Protection of Personal Data held by Private Parties. | Article 47. Pursuant to Articles 6 and 14 of the Law, the data controller has the obligation to protect and be responsible for the processing of personal data found in its custody or | Articles 63, 64 and 65 of the Federal Law on Protection of Personal Data held by Private Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | in its possession or for those it communicated to a data processor, whether or not the latter is located in Mexico. To comply with this obligation, the data controller may use standards, best international practices, corporate policies, self-regulation arrangements, or any other mechanism that it determines is adequate for such purpose.<br><br>Article 48. Pursuant to Article 14 of the Law, the data controller must adopt measures to guarantee the proper processing of personal data, giving priority to the interests of the data subject and the reasonable expectation of privacy. The measures that may be adopted by the data controller include at least the following:<br>I. Prepare privacy policies and programs that are binding and enforceable within the organization of the data controller;<br>II. Implement a program of training, updating, and raising the awareness of personnel about obligations in matters of protection of personal data;<br>III. Establish an internal supervision and monitoring system, as well as external inspections or audits to verify compliance with privacy policies;<br>IV. Dedicate resources for the implementation of privacy programs and policies;<br>V. Implement a procedure to deal | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | with the risk to the protection of personal data by the implementation of new products, services, technologies and business models, as well as to mitigate them;<br>VI. Periodically review the security policies and programs to determine modifications required;<br>VII. Establish procedures to receive and respond the questions and complaints of data subjects;<br>VIII. Have mechanisms to comply with privacy policies and programs, as well as sanctions for a breach thereof; IX. Establish measures to protect personal data, in other words, a group of technical and administrative actions that will allow the data controller to ensure compliance with the principles and obligations established by the Law and these Regulations, or<br>X. Establish measures to trace personal data, in other words, actions, measures, and technical procedures that will allow the tracing of personal data while being processed.<br><br>Article 51. The relationship between the data controller and data processor must be established by contract or other legal instrument decided upon by the data controller and that permits its existence, scope, and contents to be proven.<br>Article 52. For the processing of personal data in services, | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | applications, and infrastructure in what is called “cloud computing,” in which the data controller adheres to the same by general contractual conditions or clauses, such services may only be used when the provider: I. Complies at least with the following: a) Has and uses policies to protect personal data similar to the applicable principles and duties set out in the Law and these Regulations;<br>b) Makes transparent subcontracting that involves information about the service which is provided; c) Abstains from including conditions in providing the service that authorize or permits it to assume the ownership of the information about which the service is provided, and d) Maintains confidentiality with respect to the personal data about which it provides the service, and<br>II. Has mechanisms at least for: a) Disclosing changes in its privacy policies or conditions of the service it provides; b) Permitting the data controller to limit the type of processing of personal data about which it provides the service; c) Establishing and maintaining adequate security measures to protect the personal data about which it provides the service;<br>d) Ensuring the suppression of personal data once the service has been provided to the data controller and that the latter may recover it, and | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | e) Impeding access to personal data by those who do not have proper access or in the event of a request duly made by a competent authority, so inform the data controller.<br>In any case, the data controller may not use services that do not ensure the proper protection of personal data. For purposes of these Regulations, cloud computing shall mean the model for the external provision of computer services on demand that involves the supply of infrastructure, platform, or software distributed in a flexible manner, using virtual procedures, on resources dynamically shared. Regulatory agencies, within the scope of their authority, and assisting the Institute, shall issue guidelines for the proper processing of personal data in what is called "cloud computing."<br><br>Article 53. National and international transmissions of personal data between a data controller and a data processor need not be informed to the data subject or his consent obtained. The data processor shall be considered as a data controller, together with its own obligations, when it: I. Uses the personal data for a purpose different from that authorized by the data controller, or II. Makes a transfer without complying with the instructions of the data controller. | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | The data processor will not be held responsible when, at the express indication of the data controller, it transmits the personal data to another data processor designated by the latter, to which it had entrusted the performance of a service, or transfers the personal data to another data controller pursuant to these Regulations.<br><br>Article 67. A transfer refers to the communication of personal data to a person other than the data subject, data controller or data processor, within or outside Mexico.<br><br>Article 68. Any transfer of personal data, whether national or international, is subject to the consent of the data subject, with the exceptions provided in Article 37 of the Law; the data subject must be so informed by a privacy notice and the transfer be limited to the purposes that justify it.<br><br>Article 69. For purposes of demonstrating that the transfer, whether national or international, took place in accordance with the Law and these Regulations, the burden of proof in all cases rests upon the data controller that made the transfer and on the receiver of the personal data.<br><br>Article 70. In the case of transfers of personal data among holding | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | companies, subsidiaries, or affiliates under the common control of the same group as that of the data controller, or to a parent company or to any company belonging to the same group as that of the data controller, the mechanism to ensure that the receiver of the personal data complies with the provisions of the Law, these Regulations, and other applicable laws and regulations, may be the existence of internal rules to protect personal data whose observance is obligatory, provided that these comply with the requirements of the Law, these Regulations, and other applicable laws and regulations.<br><br>Article 71. To carry out a transfer of persona data within Mexico, it shall be necessary for the data controller to comply with the provisions of Article 36 of the Law and Article 68 of these Regulations.<br><br>Article 72. The receiver of personal data will be subject to the Law and these Regulations as a data controller and shall deal with personal data in accordance with that agreed upon in the privacy notice communicated to it by the transferring data controller.<br><br>Article 73. A transfer shall be formalized by a mechanism that allows it to be shown that the transferring data controller | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | communicated to the receiving data controller the conditions under which the data subject consented to the processing of his personal data.<br><br>Article 74. Without prejudice to the provisions of Article 37 of the Law, international transfers of personal data will be possible when the receiver of the personal data assumes the same obligations as those of the data controller transferring the personal data.<br><br>Article 75. For such purposes, a data controller that transfers personal data may use contracts and other legal instruments which contain at least the same obligations as those to which the data controller transferring personal data is subject, as well as the conditions under which the data subject consented to the processing of his personal data.<br><br>Article 76. Data controllers, if considered necessary, may request the opinion of the Institute as to whether an international transfer that they are carrying out complies with the Law and these Regulations. | | |
| | | General Law on Protection of Personal Data Held by Obligated Parties. | Article 29. The data controller must implement the mechanisms contemplated in article 30 of this Law in order to evidence compliance with the principles, duties, and obligations established in this Law and to become accountable to the data owner, the Institute or the Guarantor | Articles 163, 164 and 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | bodies, as applicable, for the processing of the personal data it holds; in order to do so, it must comply with the Constitution and the International Treaties to which Mexico is a Party. To achieve this end, it may resort to domestic or international standards and best practices insofar as these do not contravene Mexican regulations.<br><br>Article 30. Among the mechanisms the data controller must adopt to comply with the principle of responsibility established in this Law, the following are listed as an enumeration and not by way of limitation: **I.** To allocate resources authorized for such purpose to be used in the implementation of programs and policies for the protection of personal data; **II.** To develop policies and programs for the protection of personal data that are of mandatory compliance within the data controller's organization; **III.** To put into practice a training and updating program for personnel regarding the obligations and other duties in regard to personal data protection; **IV.** To review the security programs and policies regarding personal data from time to time to decide on any changes that may be required; **V.** To establish an internal | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | and/or external oversight and monitoring program, including audits, to verify compliance with personal data protection policies; **VI.** To establish the procedures for the reception and response to queries and complaints made by data owners; **VII.** To design, develop and implement its public policies, programs, services, computer systems or platforms, electronic applications or any other technology that entails the processing of personal data, in accordance with the provisions set forth in this Law and such others that may be applicable on the matter; and **VIII.** To ensure that its public policies, programs, services, computer systems or platforms, electronic applications or any other technology that entails the processing of personal data comply automatically with the obligations contemplated in this Law and in other applicable provisions on the matter.<br><br>Article 65. All transfers of personal data, whether domestic or international, are subject to the data owner's consent, except for the | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | exceptions contemplated in articles 22, 66 and 70 of this Law.<br><br>Article 66. All transfers must be formalized by the execution of contractual clauses, collaboration agreements or any other legal instrument, in adherence to the regulations applicable to the data controller, that provide evidence on the scope of the processing of the personal data, as well as on the obligations and responsibilities undertaken by the parties.<br><br>The provisions of the foregoing paragraph will not apply in the following cases: I. When involving a domestic transfer taking place between data controllers to comply with a legal provision, or when the data controllers are exercising attributions expressly conferred upon them; or II. When involving an international transfer which is contemplated in a law or treaty signed and ratified by Mexico; or else, when it takes place at the request of a foreign authority or competent international body acting as recipient, provided the faculties of the transferring data controller and the recipient are equivalent; or else, when the ends for which the transfer takes place are analogous to or compatible with those that gave rise | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | to processing by the transferring data controller.<br><br>Article 67**.** When the transfer involved is domestic, the personal data recipient must process the personal data, undertake the commitment to ensure their confidentiality and use them solely for the purposes for which they were transferred, while adhering to the provisions of the privacy notice of which the transferring data controller must make it cognizant.<br><br>Article 68. The transfer or transmittal of personal data outside the Mexican territory by the data controller can only take place when the third party recipient or data processor undertakes to protect such data in adherence to the principles and duties established in this Law and the applicable provisions on the matter.<br><br>Article 69. The data controller must, when making any transfer of personal data, provide the personal data recipient with the privacy notice governing the processing of the data owner's personal data.<br><br>Article 70. The data controller may transfer personal data without the need of obtaining the data owner's | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | consent in the following cases: I. When such transfer is contemplated in this Law or other statutes, international agreements or Treaties signed and ratified by Mexico; II. When transfer is between data controllers, provided the personal data are used in the exercise of their own faculties as are compatible with or analogous to the purposes that gave rise to the processing of the personal data; III. When transfer is legally ordered in the investigation and prosecution of crimes as well as for purposes of law enforcement and the administration of justice; IV. When transfer is required to uphold, exercise or defend a right before the competent authority, provided transfer has been requested by such authority; V. When transfer is required for health prevention or medical diagnosis, to provide health care, medical treatment or for the management of health care services, provided evidence of this requirement is provided; VI. When transfer is required to preserve or comply with the legal relationship between the data controller and the data owner; VII. When transfer is required under a contract executed or to be executed by the data controller and a third party in the data owner's interest; VIII. When involving the cases in which the data | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | controller is not under the obligation of obtaining the data owner's consent for processing and transmission of his/her personal data, as provided in article 22 of this Law; or IX. When the transfer is required for reasons of national security.<br><br>Action by the data controller falling within the exceptions contemplated in this article does not preclude its compliance with applicable obligations set forth in this Chapter. | | |
| | | General Guidelines of Protection of Personal Data Held by Obligated Parties. | Articles 46 to 50 describe the data controller obligation to adopt and implement policies, mechanisms and activities (including programs for data protection and training as well as supervision and monitoring systems) to assure the compliance of the principles, duties and other data protection obligations provided in the law. These articles also provide the obligation of the data controllers to stablish procedures to address complaints filed by data subjects.<br><br>Articles 51 and 52 provide data protection measures of privacy by default and by design that must be taken into account by data controllers.<br><br>Articles 113 to 118 describe general conditions for personal data | Articles 163, 164 and 165 of the General Law on Protection of Personal Data Held by Obligated Parties | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | transfers such as that they have to be informed by the data controller to the data subject in the privacy notice and, as the case may be, consented by him; mechanisms to request the express consent for transfers; characteristics and requirements of national and international transfers and the possibility to ask for the opinion of the national data protection authority regarding international transfers to be realized. | | |
| **C** | **Domestic Implementation** | | | | |
| | ***Giving Effect to the Framework - Establishment of a Privacy Enforcement Authority*** **(Ref. Para. 41)** Member Economies should consider establishing and maintaining Privacy Enforcement Authorities which are provided with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis. | DECREE by means of which several provisions of the Mexican Constitution are amended in transparency matters, published in the Federal Official Gazette, on February 7, 2014. | Article 6, section A. subsection VIII of the Mexican Constitution:<br><br>The Federation shall establish an autonomous, specialized, impartial and collegiate agency. It must have a legal personality; own assets; full technical, managerial and decision power over its budget and internal organization; and shall be responsible for guaranteeing the fulfillment of the right of access to public information and the protection of personal data held by public agencies (obligated subjects), according to the terms established by law.<br><br>The autonomous transparency agency established in this fraction will be governed by the transparency and access to public information law, as well as the law for the protection on personal data held by obligated subjects, in the terms established by | N/A | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | the general law issued by the Congress to set the basic principles, basis and procedures for the exercise of the information rights.<br><br>This agency will be governed by the principles of certainty, legality, independence, impartiality, efficiency, objectiveness, professionalism, transparency and maximum publicity.<br><br>The autonomous transparency agency has competence to receive inquiries related to the right of access to public information and the protection of personal data from any authority, entity, organism or agency that belongs to any of the Executive, Legislative or Judicial Powers, as well as any autonomous agency, political parties public trusts and public funds, or any other person, group, union or organization that receives or use public resources or that exercise authority at the federal domain with exception of those issues that correspond to the jurisdiction of the Federal Supreme Court, in which case a committee of three Supreme Court Justices would decide the issue. The autonomous transparency agency has, also the competence to receive the inquiries from individuals in regard to the resolutions issued by the local autonomous specialized transparency agencies and the | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | Federal District transparency agency that ruled the inexistence, reserve, and confidentiality of information or that refuses to disclose information according to the terms established by law.<br><br>The National Transparency Agency [organismo garante], ex oficio or by substantiated petition of the local agency from the States or the Federal District may receive or analyze the inquiries that due to its importance or transcendence are in the interest of the National Transparency Agency.<br>The law will determine the information that shall be considered as reserved or confidential.<br><br>The resolutions of the National Transparency Agency are mandatory, definitive and indisputable for the obligated subjects (obligors). Only in the cases that the resolutions may be considered to endanger public security according to the law in the matter, the Legal Councilor of the Federal Government may present a review inquiry to the Supreme Court.<br><br>The National Transparency Agency [organismo garante] shall be constituted by seven commissioners. To appoint them, the Senate, previous extensive | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | consultation to social actors and by proposal of the different parliamentary groups, will appoint the commissioner with the vote of two-thirds of the Senators present in the session according to the vacancy that must be covered and following the procedure established by law. The President may oppose the appointment within ten business days. If the President does not oppose the appointment within the given days, then the person appointed by the Senate will assume the commissioner office.<br><br>Given the case that the President opposes the appointment, the Senate will present a new proposal to occupy the vacancy according to the previous paragraph. However, to approve the proposal the vote of three-fifths of the Senators present is required. If this second appointment were objected, the Senate, according to the procedures in the previous paragraph, with the approval of three-fifths of the Senators present would appoint definitively the commissioner that will occupy the vacancy.<br><br>The commissioner office will be held during seven years, and the commissioners shall fulfill the requirements provided in the fractions I, II, IV, V and VI of the article 95th of this Constitution. The | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | commissioners shall not hold other office, have an additional employment, or other commission with exception of the non-profit chairs or offices related to charities and academic or scientific institutions. The commissioners can only be removed from office according to the terms in the Fourth Title of this Constitution and they will be subject to political trial.<br><br>The conformation of the National Transparency Agency shall promote gender equality.<br><br>The Commissioner President shall be selected by a peer process, through the secret vote of the commissioners. The Commissioner President will remain in office for three years, with the possibility of being reelected to other three years. The commissioner president must render an annual report before the Senate in the date and terms described by the law.<br>The National Transparency Agency [órgano garante] shall have an Advisory Board, formed with ten council members that shall be elected by the vote of two thirds of the present Senators. The law will establish the procedures to present the proposals to the Senate. Each year, the two council members with longer tenure will be replaced, | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | unless they were proposed and ratified for a second term in office.<br><br>The law will establish the emergency measures and procedures that the Agency could implement to guarantee the fulfillment of its decisions.<br><br>Every authority and public servant is compelled to help the National Transparency Agency and its Commissioners for the adequate performance of the Agency.<br><br>The National Transparency Agency will coordinate its actions with the Federal Superior Comptroller Office [Entidad de Fiscalización Superior de la Federación], the entity specialized in archives and files, the organ in charge of gathering and process of statistical and geographical data, as well as, with the local agencies in the States and the Federal District in order to strengthen the accountability within the Mexican State.<br><br>Likewise, transitory article seven of the Decree provides that the same authority abovementioned (article 6, section A, subsection VIII of the Mexican Constitution) will have the power to address issues regarding personal data protection held by | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | private parties as long as there is no other authority determined to do so. | | |
| | ***Privacy Management Programmes*** **(Ref. Para. 44)** Member Economies should consider encouraging personal information controllers to implement privacy management programmes that: (i) are tailored to the structure and scale of their operations, and the volume and sensitivity of the personal information under their control; (ii) provide appropriate safeguards based on risk assessment that takes into account the potential harm to individuals; (iii) are integrated into accountable governance structures with appropriately trained personnel and establish internal oversight mechanisms; (iv) include mechanisms for responding to inquiries and incidents; (v) are updated in light of ongoing monitoring and periodic assessment. | Federal Law on Protection of Personal Data held by Private Parties.<br><br>Regulations to the Federal Law on Protection of Personal Data held by Private Parties. | Article 14. The data controller shall ensure compliance with the personal data protection principles established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller. The data controller must take all necessary and sufficient action to ensure that the privacy notice given to the data owner is respected at all times by it or by any other parties with which it has any legal relationship.<br><br>Article 48. Pursuant to Article 14 of the Law, the data controller must adopt measures to guarantee the proper processing of personal data, giving priority to the interests of the data subject and the reasonable expectation of privacy.<br><br>The measures that may be adopted by the data controller include at least the following: I. Prepare privacy policies and programs that are binding and enforceable within the organization of the data controller; II. Implement a program of training, updating, and raising the awareness | Articles 163, 164 and 165 of the General Law on Protection of Personal Data Held by Obligated Parties | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | of personnel about obligations in matters of protection of<br><br>personal data; III. Establish an internal supervision and monitoring system, as well as external inspections or audits to verify compliance with privacy policies; IV. Dedicate resources for the implementation of privacy programs and policies; V. Implement a procedure to deal with the risk to the protection of personal data by the implementation of new products, services, technologies and business models, as well as to mitigate them; VI. Periodically review the security policies and programs to determine modifications required; VII. Establish procedures to receive and respond the questions and complaints of data subjects; VIII. Have mechanisms to comply with privacy policies and programs, as well as sanctions for a breach thereof; IX. Establish measures to protect personal data, in other words, a group of technical and administrative actions that will allow the data controller to ensure compliance with the principles and obligations established by the Law and these Regulations, or X. Establish measures to trace personal data, in other words, actions, measures, and technical procedures that will allow the tracing | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | of personal data while being processed.<br><br>Article 61. In order to establish and maintain the security of personal data, the data controller must take into account the following actions: I. Prepare an inventory of personal data and processing systems; II. Determine the duties and obligations of those who process personal data;<br><br>III. Have a risk analysis of personal data consisting of identifying dangers and estimating the risks to the personal data; IV. Establish the security measures applicable to personal data and identify those implemented effectively; V. Analyze the gap between existing security measures and those missing that are necessary for the protection of personal data; VI. Prepare a work plan for the implementation of the missing security measures arising from the gap analysis; VII. Carry out reviews and audits; VIII. Train personnel who process personal data, and IX. Keep a record of personal data storage media.<br><br>The data controller shall prepare a document setting out security measures arising from the previous paragraphs. | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | Parameters for personal data self-regulation | Article 62. Data controllers must update the document setting out security measures when the following events occur: I. Modifications to the security measures or processes are made for their continuous improvement, arising from revisions of the security policy of the data controller; II. Substantial modifications are made in the processing arising from a change in the level of risk; III. Processing systems are violated, as provided in Article 20 of the Law and Article 63 of these Regulations, or IV. There is an impact upon the personal data other than the above.<br><br>In the case of sensitive personal data, the data controller shall review, and if necessary update the security document once a year.<br><br>Articles 15 to 37 of the Parameters for personal data self-regulation provide the establishment of a personal data management system as an important element of self-regulation schemes, in order for them to be recognized by the national data protection authority. Some of the features of such personal data management system include: a personal data management policy; support of the top executives; designation of the personnel in charge of the | Chapter I, section I of the Parameters for personal data self-regulation<br><br>The adoption of privacy of self-regulation schemes is a voluntarily decision of data controllers. Notwithstanding the above, the compliance of such schemes, once adopted, is binding and must be sanctioned by measures imposed by the data controllers themselves. | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | management system and training for such personnel; assignment of functions and responsibilities; an inventory of personal data; risk analysis; training of staff related to any personal data processing; development and implementation of specific procedures to comply with the data protection principles, duties and obligations; actions to continuously update the system; plans, implementation and up-date of an audit program; plan, implementation and maintenance of administrative reviews; preventive and corrective measures and consequences for non-compliance, as well as measures to assure a continuous effectiveness of the system. | | |
| | | General Law on Protection of Personal Data Held by Obligated Parties. | Article 34. The actions relating to the personal data processing security measures must be documented and kept in a management system.<br>A management system will be understood to be the set of interrelated elements and activities set up to establish, implement, operate, monitor, review, maintain and improve the processing and security of personal data, in accordance with the provisions of | Articles 163, 164 and 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | this Law and other applicable provisions on the matter.<br><br>Article 35. In particular, the data controller must prepare a security document containing, at least, the following: **I. The inventory on the personal data and the processing systems; II.** The functions and duties of the persons involved in the processing of personal data; **III.** Risk analysis; **IV.** Gap analysis; **V. Work plan; VI.** The monitoring and review mechanisms regarding security measures; and **VII.** The general training program.<br><br>Article 36. The data controller must update the security document whenever any of the following events occurs: **I.** Substantial changes in the processing of the personal data are made that entail a change in risk level; **II.** As a result of a continuing improvement process, arising from the monitoring and review of the management system; **III.** As a result of an improvement process intended to mitigate the impact of a security breach that may have occurred; and<br>**IV.** After the implementation of corrective and preventive measures as a result of a security breach. | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | Article 37. Should a security breach occur, the data controller must analyze the causes that gave rise to it and include in its work plan the preventive and corrective actions required to adapt the security measures and the personal data processing, such being the case, so as to prevent the breach from occurring again.<br><br>Article 38. In addition to those specified in the relevant laws and in applicable regulations, any of the following events, listed here as a minimum, are considered to be security breaches at any phase in the processing of personal data: **I.** Loss or unauthorized destruction; **II.** Theft, misplacement or unauthorized copying; **III.** Unauthorized use, access or processing; and **IV.** Damage to and unauthorized alteration or modification.<br><br>Article 39. The data controller must keep a logbook to record security breaches, which must include a description of same, date of occurrence, their causes and the corrective measures that were | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | implemented forthwith and definitively. | | |
| | | General Guidelines on Protection of Personal Data Held by Obligated Subjects. | Article 65 provides that any data controller from the federal public sector shall implement a security management system in order to plan, establish, implement, operate, monitor, maintain, review and improve security administrative, physical and technical measures to protect personal data, taking into consideration national and international standards in the matter. | Articles 163, 164 and 165 of the General Law on Protection of Personal Data Held by Obligated Parties. | |
| | ***Promotion of Technical Measures to Protect Privacy*** **(Ref. Para. 46)**<br>When considering approaches to give effect to the Framework, Member Economies should promote technical measures which help to protect privacy. | See privacy protection scheme in principle VII Security safeguards.<br><br>Additionally, the National Data Protection Authority has developed the following:<br>-Recommendations on security of personal data, published in the Official Gazette in 2013.<br>-Guide to implement a Management System for the Security of Personal Data;<br>-Handbook of security of personal data for MSMEs and small organizations;<br>-Functional equivalence table between information security standards and the Data Protection Law, Regulations and the Recommendations on security of personal data; | See provisions in principle VII Security safeguards.<br><br>Additionally, article 39, section V, of the Federal Law of Protection of Personal Data held by private parties, provides that the National Data Protection Authority has the power to disseminate international best practices and standards for information security, in view of the nature of the data, the processing purposes, and the technical and financial capacity of the data controller.<br><br>Likewise, article 89, section XIII, of the General Law for Protection of Personal Data held by Obligates subjects provides that a National Data Protection Authority has the power to publicize and issue recommendations, standards and | See sanctions in principle VII security safeguards. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | -Guide for the Secure Erasing of Personal Data, and<br>-Recommendations for the handling of personal data security incidents. | best practices on the matters subject to regulation under this Law. | | |
| | ***Public Education and Communication***<br>**(Ref. Para. 48)**<br>Member Economies should:<br>(a) publicize how their Privacy Laws and other domestic arrangements provide privacy protections to individuals; and (b) engage in activities that raise awareness amongst personal information controllers and processors about their responsibilities and obligations. | Federal Law on the Protection of Personal Data held by private parties | Article 38. The Institute, for the purposes of this Law, will have the purpose of disseminating information on the right to personal data protection in Mexican society, promoting its exercise, and overseeing the due observance of the provisions of this Law and those arising hereof; particularly those related to the fulfillment of obligations by the parties regulated by this Law.<br><br>Article 39, section XI, provides that the National Data Protection Authority has the power to develop, promote and disseminate analyses, studies and research in the area of protection of personal data held by third parties and provide training to the obligated parties, | N/A | Enacted |
| | | General Law on the Protection of Personal Data held by Obligated Parties. | Article 89, section XIII, provides that a National Data Protection Authority has the power to publicize and issue recommendations, standards and best practices on the matters subject to regulation under this Law. | N/A | Enacted |
| | | Additionally, INAI as the National Data Protection Authority has developed the following guides and documents, among others: | | N/A | N/A |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | For individuals (data subjects):<br>-Guide for data subjects.<br>-Interactive guide for data subjects.<br>-Guide to prevent identity theft.<br>-Procedure to exercise ARCO rights.<br>-Recommendations to keep privacy and personal data secure in the digital environment.<br>-Test: How do you protect yourself in the digital environment?<br>-Guide for privacy settings on social networks.<br>-Parental supervision tool guide<br>-Material on protection of personal data for educators.<br>For controllers (public sector):<br>- Brief guide for obliged subjects to contract computer services in the cloud that involve the processing of personal data.<br>-Recommendations for obliged subjects in the appointment of the personal data protection officer.<br>-Recommendations for the handling of personal data security incidents.<br>-Recommendations to recognize the main threats to personal data based on the risk assessment.<br>-Conformity of accession contracts for computer services in the cloud vs | | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | the minimum criteria for the contract of computer services in the cloud that involve the processing of personal data.<br>-Guide for the processing of biometric data.<br>-Recommendations on the protection of personal data contained in the credential to vote.<br>-Personal data protection program.<br>-The ABC of privacy notice (public sector).<br>-Guide to comply with the principles and duties of the General law on the protection of personal data in possession of obligated subjects.<br>-Guide for the preparation of the privacy notice in the area of human resources (public sector).<br>-Recommendations to guide the due processing of personal data in the register of access control to buildings and facilities of the obligated subjects.<br>-Guide to instrument countervailing measures in the public sector.<br>-Recommendations on the processing of personal data in the clinical records of public health institutions.<br>-Guide for the protection of personal data with a perspective of | | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | documentary management and archives.<br>-Recommendations for data subjects in the labor field for the public sector.<br>-Brief guide for obliged subjects for contracting cloud computing services that involve the processing of personal data.<br>-Brief guide for obliged subjects for contracting cloud computing services that involve the processing of personal data.<br><br>-Practical Guide to address requests for the exercise of ARCO rights;<br>-Recommendations for the designation of the person or Department in charge of Personal Data Protection;<br>-ABC guide for Privacy Notices;<br>-Self-Evaluation template of Privacy Notices for the Private Sector;<br>-Short Privacy Notice Model for Video Surveillance;<br>-Privacy Notice Generator for Private Sector;<br>-Guide to implement compensatory measures;<br>-Privacy Notice Models for immigrants;<br>-Guide to comply with the principles and duties of the Federal Law of | | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | Protection of Personal Data held by Private Parties;<br>-Guide to assist data controllers in the correct processing of personal data in the extrajudicial collection;<br>-Self-Evaluation template of Privacy Notice for the Public Sector;<br>-*Corpus Iuris* in the protection of personal data;<br>-Procedure to exercise the ARCO rights before the public entities;<br>-Recommendations on protection of personal data in the ID card;<br>-Guide for the processing of biometrics;<br>- Privacy Notice Generator for Public Sector;<br>-Guide to prevent the identity theft;<br>-Television serie *Monsters Online*;<br>-Data Subjects Guide of Personal Data Protection, and<br>-Recommendations to maintain privacy and security of personal data in the digital environment.<br>-Recommendations to recognize the main threats to personal data from risk assessment.<br>-Guide for self-regulatory schemes regarding the protection of personal data | | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | -Guide for development privacy impact assessments<br>-Personal data security Awareness Toolkit for private sector<br><br>The ways to publicize are: the official site of the National Institute of Transparency, Access to Information and Data Protection or INAI (the National Data Protection Authority in Mexico) - https://home.inai.org.mx/; official communications; social networks, broadcasting and specialized media, as well as data protection events and contests (in privacy innovation GPA participation and others).<br>*Corpus Iuris* in the protection of personal data: http://corpusiurispdp.inai.org.mx/Pages/home.aspx<br><br>Applicable and current law is published and available for public consultation at INAI website: https://home.inai.org.mx/?page_id=1870&mat=p<br><br>And also through National Transparency Platform (PNT) website:<br><br>https://consultapublicamx.inai.org.mx/vut- | | | |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | web/faces/view/consultaPublica.xhtml#inicio<br><br>Also available for consultation in Congress and Official Gazette websites.<br>http://www.diputados.gob.mx/LeyesBiblio/index.htm<br><br>http://www.dof.gob.mx/ | | | |
| | ***Cooperation Within and Between Public and Private Sectors***<br>**(Ref. Para. 49, 51)**<br>Member Economies should seek the cooperation of non-government stakeholders in furthering the Framework's objectives.<br>Member Economies should consider developing strategies that reflect a coordinated approach to implementing privacy protections across governmental bodies. | Federal Law on Protection of Personal Data held by Private Parties. | Article 58. Data owners who feel they have suffered harm or damage to their property or rights as a result of a breach of the provisions of this Law by the data controller or data processor, may exercise<br><br>Regarding the notification of data breaches, see provisions referred to in principle VII security safeguards. | N/A | Enacted |
| | | General Law on Protection of Personal Data Held by Obligated Parties | Article 89. In addition to the powers conferred upon the Institute under the General Law on Transparency and Access to Public Information, the Federal Law on Transparency and Access to Public Information and other regulations as may be applicable; it will have the following attributions: […] XII. Providing technical support to data controllers in complying with the obligations set forth in this Law; […] XX. Entering into agreements with data controllers to develop programs intended to | N/A | Enacted. |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | | harmonize the processing of personal data in specific sectors, enhancing the protection of personal data, and undertaking any improvements regarding practices in this matter; […] XXIII. Entering into agreements with the Guarantor bodies that will contribute to the achievement of the objectives contemplated in this Law and other applicable provisions on the matter; […] XXX. Cooperating with other oversight authorities and domestic and international organizations, in order to provide assistance in the matter of personal data protection, in accordance with the provisions of this Law and other applicable regulations. | | |
| | | Additionally, the National Data Protection Authority has signed several collaboration agreements with commercial chambers and associations. | N/A | N/A | N/A |
| | ***Appropriate Remedies where Privacy Protections are Violated*** **(Ref. Para. 53, 54)** A Member Economy's system of privacy protections should include appropriate remedies for privacy violations, which could include redress, the ability to stop a violation from continuing, and | Federal Law on Protection of Personal Data held by Private Parties. | Article 58 Data owners who feel they have suffered harm or damage to their property or rights as a result of a breach of the provisions of this Law by the data controller or data processor, may exercise<br><br>Regarding the notification of data breaches, see provisions referred to in principle VII security safeguards. | Regarding the notification of data breaches, see sanctions referred to in principle VII security safeguards. | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | other remedies.<br>Member Economies should consider encouraging or requiring personal information controllers to provide notice, as appropriate, to Privacy Enforcement Authorities and/or other relevant authorities in the event of a significant security breach affecting personal information under its control. Where it is reasonable to believe that the breach is likely to affect individuals, timely notification directly to affected individuals should be encouraged or required, where feasible and reasonable. | General Law on Protection of Personal Data Held by Obligated Parties | Article 165. Any responsibility that is established under the relevant administrative proceedings, arising from the infringement of the provisions of article 163 of this Law, is independent from any civil, criminal or other liabilities which may arise from the same actions.<br><br>Said responsibilities and liabilities will be determined independently, through the proceedings contemplated in applicable laws; and the sanctions which are imposed by the competent authorities, such being the case, will also be enforced independently. […]<br><br>To these ends, the Institute or the Guarantor bodies may denounce before the competent authorities any action or omission that is in violation of this Law, and submit the evidence considered to be pertinent, as provided in applicable laws.<br><br>Regarding the notification of data breaches, see provisions referred to in principle VII security safeguards. | Regarding the notification of data breaches, see sanctions referred to in principle VII security safeguards. | Enacted. |
| | **International Implementation** | | | | |
| | ***Cross-Border Cooperation in Investigation and Enforcement*** **(Ref. Para.62)**<br>Member Economies should expand their use of existing cooperative arrangements and | Federal Law on Protection of Personal Data held by Private Parties. | Article 39. The Institute has the following responsibilities: […] VII. Cooperate with other domestic and international bodies and supervisory authorities, in order to assist in the area of data protection, and […] IX. | N/A | Enacted |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | consider developing additional cooperative arrangements or procedures, as necessary, to facilitate cross-border cooperation in the enforcement of privacy laws. | | Participate in international fora in the area of this Law; […]. | | |
| | | General Law on Protection of Personal Data Held by Obligated Parties | Article 89. In addition to the powers conferred upon the Institute under the General Law on Transparency and Access to Public Information, the Federal Law on Transparency and Access to Public Information and other regulations as may be applicable; it will have the following attributions: […] XXX. Cooperating with other oversight authorities and domestic and international organizations, in order to provide assistance in the matter of personal data protection, in accordance with the provisions of this Law and other applicable regulations. | N/A | Enacted |
| | | Mexico has joined the following investigation and international cooperation agreements and mechanisms:<br>- GPEN;<br>- CPEA, and<br>- -Convention for the protection of individuals with regard to automatic processing of personal data and Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows<br>- Global Privacy Enforcement Network (GPEN);<br>- APEC Cross-border Privacy Enforcement Arrangement (CPEA) | N/A | N/A | N/A |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | | - USMCA (Chapter 19 on Digital Commerce and 19.14 on Cooperation).<br>-<br>Additionally, Mexico and the United States are working on cross-border data flows with the High-Level Economic Dialogue | | | |
| | ***Cross-Border Privacy Mechanisms***<br>**(Ref. Para. 66)**<br>Member Economies will endeavor to support the development and recognition or acceptance of cross-border privacy mechanisms for use by organisations to transfer personal information across the APEC region, recognizing that organizations would still be responsible for complying with local privacy requirements as well as with all applicable laws. | Mexico joined the CBPR System in 2013.<br>Mexico, the United States and Canada are promoting the adoption of the CBPR System among the private sector in North America region thorough Chapter XIX of the UMSCA. | N/A | N/A | N/A |
| | ***Cross-Border Transfers***<br>***(Ref. Para. 69)***<br>A Member Economy should restrain from restricting cross-border flows of personal information between itself and another Member Economy where:<br>(a) The other Economy has in place legislative or regulatory instruments that give effect to the | See privacy protection schemes regarding principle IX Accountability and personal data transfers. | See provisions regarding principle IX Accountability and personal data transfers. | See sanctions regarding principle IX Accountability. | Enacted. |

| | APEC Principle / Commentary / Implementation guidance | Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1] | Provision[2] | Sanction[3] | Results/ Status[4] |
|---|---|---|---|---|---|
| | Framework; or<br>(b) sufficient safeguards exist including effective enforcement mechanisms and appropriate measures (such as the CBPR) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it. | Mexico, together with the United States of America are working to strengthen cross-border data flows and interoperability between privacy legislations through the US - Mexico High-Level Economic Dialogue. | | | |
| **D** | ***Network point of contact arrangements[7]*** | Contact details will be made available to APEC members through the APEC Secretariat. | | | |

[7] Please provide contact details such as name and/or title, address, telephone and email contacts. This information will not be published but will be made available to Member Economies.